NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBERSPACE ACTIONS IN A COUNTERINSURGENCY

by

Andrzej V. Kujawski

June 2016

Thesis Advisor: Wade Huntley
Second Reader: Pablo Breuer

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE CYBERSPACE ACTIONS IN A COUNTERINSURGENCY			**5. FUNDING NUMBERS**
6. AUTHOR(S) Andrzej V. Kujawski			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This work addresses the insufficiency of United States Department of Defense joint doctrine for incorporating cyberspace operations into counterinsurgency (COIN) campaigns. This insufficiency is addressed through the use of a matrix, which aligns the cyberspace actions described in joint cyberspace doctrine against the COIN tenets outlined in joint COIN doctrine. Each intersection of cyberspace actions and COIN tenets is explored, first by listing the effects that the cyberspace action can produce in support of the COIN tenet. Each list of effects is then evaluated to determine the degree to which these effects are accounted for by current doctrine, whether these effects have been seen in actual COINs, and how significantly these effects contribute to a COIN campaign. To facilitate open discussion, we draw only from unclassified sources. We find that existing doctrine does not address many types of missions and operations that can produce effects in support of the COIN tenets. The intersections with effects that contribute most significantly to a COIN campaign, but are least accounted for by current doctrine, are prioritized; we then propose additions to current doctrine that account for the insufficient guidance. We conclude by addressing the limitations of this mapping and suggesting future research.

14. SUBJECT TERMS counterinsurgency, cyber, doctrine			**15. NUMBER OF PAGES** 119
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CYBERSPACE ACTIONS IN A COUNTERINSURGENCY

Andrzej V. Kujawski
Captain, United States Army
B.A., University of San Diego, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2016

Approved by: Wade Huntley, PhD
Thesis Advisor

CDR Pablo Breuer
Second Reader

Cynthia Irvine, PhD
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This work addresses the insufficiency of United States Department of Defense joint doctrine for incorporating cyberspace operations into counterinsurgency (COIN) campaigns. This insufficiency is addressed through the use of a matrix, which aligns the cyberspace actions described in joint cyberspace doctrine against the COIN tenets outlined in joint COIN doctrine. Each intersection of cyberspace actions and COIN tenets is explored, first by listing the effects that the cyberspace action can produce in support of the COIN tenet. Each list of effects is then evaluated to determine the degree to which these effects are accounted for by current doctrine, whether these effects have been seen in actual COINs, and how significantly these effects contribute to a COIN campaign. To facilitate open discussion, we draw only from unclassified sources. We find that existing doctrine does not address many types of missions and operations that can produce effects in support of the COIN tenets. The intersections with effects that contribute most significantly to a COIN campaign, but are least accounted for by current doctrine, are prioritized; we then propose additions to current doctrine that account for the insufficient guidance. We conclude by addressing the limitations of this mapping and suggesting future research.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFDD	Air Force Doctrine Document
ALAT	Assistant Legal Attaché
ASCOPE	area, structures, capabilities, organizations, people and events
BRIC	Brazil, Russia, India, China
C2	command and control
CAUSE	Cyber-attack Automated Unconventional Sensor Environment
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CIA	Central Intelligence Agency
CO	cyberspace operations
COCOM	combatant commander
COIN	counterinsurgency
CSE	cyber support element
DCO	defensive cyber operations
DDOS	distributed denial of service
DIME	Diplomatic, Informational, Military, Economic
DISA	Defense Information Systems Agency
DNS	Domain Name Service
DOD	Department of Defense
DODIN	Department of Defense Information Network
FARC	Fuerzas Armadas Revolucionarias de Colombia
FBI	Federal Bureau of Investigation
FM	field manual
HN	host nation
IARPA	Intelligence Advanced Research Projects Activity
IGL	intelligence gain / loss
IO	information operations
IPB	intelligence preparation of the battlefield
ISIS	Islamic state in Syria
ISP	Internet service provider
JFC	joint forces commander
JFHQ-C	joint forces headquarters-cyber

JISM	Jordan Institute for Standards and Metrology
JP	Joint Publication
JMEM	Joint Munitions Effectiveness Manual
JTF	joint task force
LOE	Line of Effort
LOO	Line of Operation
MCO	Marine Corps Order
MCP	Malaysia Communist Party
MENA	Middle East and North Africa
MISO	military information support operations
MOE	Measure of Effectiveness
MOP	Measure of Performance
NATO	North Atlantic Treaty Organization
NGO	non-governmental organization
NIST	National Institute of Standards and Technology
OCO	offensive cyber operations
OE	operational environment
OGO	other governmental organization
OIG	Office of the Inspector General
OPE	operational preparation of the environment
OPM	Office of Personnel Management
PIR	priority information request
PMESII-PET	Political, Military, Economic, Social, Infrastructure, Information, Physical Environment, and Time
PSYOPS	psychological operations
SECNAV	Secretary of the Navy
SOF	special operations forces
STIG	security technical implementation guide
TOR	the Onion router
TTP	tactics, techniques, and procedures
US	United States
USD-ATL	Undersecretary of Defense – Acquisition, Technology, and Logistics
USJCS	United States Joint Chiefs of Staff

ACKNOWLEDGMENTS

I would like to thank Dr. Wade Huntley and Commander Pablo Breuer for their assistance with this work. Their combined input of outstanding academic and operational experience provided me with multiple perspectives and sources of inspiration.

This work is dedicated to my wife, Mary Ellen. Her constant love and support provided me with the time and energy I needed to achieve my academic goals. She and my son, Ryan, are the reasons why I do what I do.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. TRENDS IN THE UNITED STATES' NEAR FUTURE CONFLICTS

The United States in future years will likely be engaged in few if any high-intensity conflicts, but in many small wars and COINs (National Intelligence Council 2012, 59–62). Many also predict that the role of information technology will increase in both shaping and fighting these wars (National Intelligence Council 2012, 83–87). In recent years, the Department of Defense (DOD) has rewritten its counterinsurgency manual, and has published its first doctrine on how to incorporate cyberspace operations into military operations in general. Current United States COIN doctrine does not fully integrate the wide range of cyberspace actions and effects that can contribute to COINs. It provides guidance that closely matches the intent-based division of cyberspace operations provided by United States cyberspace operations doctrine, but does not address the effects-based division which cyberspace operations doctrine also provides. Current United States COIN doctrine fails to provide as much guidance on cyberspace operations as it does for other supporting operations with respect to both the effects that cyberspace operations can achieve, and how these effects contribute to accomplishment of the COIN tenets.

B. PURPOSE OF THIS THESIS

This work examines the current state of United States military doctrine with regard to incorporation of cyberspace actions and effects into COIN campaigns. If current doctrine is sufficient, then there should be little to gain from adding or changing current doctrine. If current doctrine is not sufficient, then the opportunity exists to contribute to or modify doctrine in such a way that the United States is better able to incorporate cyberspace operations into future COIN campaigns. This work determines whether current doctrine is sufficient by creating and exploring a matrix that aligns the effects-based division of cyberspace operations described in Joint Publication (JP) 3–12(R), Cyberspace

Operations, with the COIN tenets described in JP 3–24, Counterinsurgency. This paper refers to this alignment process as a mapping, and uses this mapping to evaluate how well current doctrine addresses the effects that these cyberspace actions can contribute to accomplishment of the COIN tenets.

C. METHODOLOGY

This research uses a matrix format to illustrate how each cyberspace action can achieve effects that contribute to the accomplishment of each COIN tenet. We then examine the degree to which current doctrine sufficiently addresses these effects, and analyze the significance of these effects based on case examples from actual COINs, and how significant a contribution these effects have made or may have made, had they been achieved. Next, we categorize and prioritize the cells based on the degree to which doctrine sufficiently addresses these effects and the degree to which these effects contribute to accomplishment of the COIN tenets. Finally, we recommend additions to future doctrine that address the cells with the most significant or most easily addressed doctrinal insufficiencies.

There are two components of this thesis that impact the manner in which our mapping is constructed and evaluated. First, our mapping is created around doctrinal terms that have only recently been codified in doctrine and are not uniformly interpreted or applied across the DOD. This lack of uniformity is equally true for any terminology used in the burgeoning field of cyberspace operations, and to a lesser degree in the politically relevant field of COIN. Among the many contested terms to choose from as the basis of this mapping, this thesis uses terminology drawn directly from the joint doctrine that drives both cyberspace and COIN operations. Second, we draw case examples from open-source information. The full impact of this decision is discussed in Chapter IV. Although there may be classified information available that would discredit or further credit the findings of this thesis, our second choice ensures that this thesis may be shared and discussed by a larger audience.

D. BACKGROUND

A growing body of work has addressed this absence in doctrine of how cyberspace actions and effects can contribute to COINs. These works can be grouped in three different bodies: those that argue the United States cannot provide guidance on cyberspace operations' contributions to COINs, those that provide guidance on cyberspace operations' contributions to one or two COIN tenets, and those that provide guidance on one or two cyberspace actions' contributions to COIN generally.

1. Works that Doubt the United States' Ability to Provide Guidance on Cyberspace Operations' Contributions to COINs

Some have claimed that the absence of guidance on applying cyberspace operations in a COIN is inevitable, because cyberspace actions cannot be conducted against modern insurgent groups. They base this claim either on the nature of the conflict or on the limitations of United States political or military leadership.

Those who claim that this absence of guidance is inevitable and due to the nature of the conflict argue that "taking the offensive may itself be in doubt as limiting war to cyber space may make the principle of offense less obvious. The roles of offense and defense seem to blur within an insurgency model as they do within cyber space" (Liles, Rogers, Dietz, and Larson 2012, 176). These claims often stem from the inability to attribute cyberspace activity to specific actors, as Jasper does by stating, "technical properties of cyberattack vectors that prevent attribution allow actors to operate with near anonymity and impunity" (Jasper 2015, 62). In this context, some have claimed that the best method of deterring malicious cyberspace activity at this time may be through "non-cyber, whole-of-nation, and whole-of-government means" (Trujillo 2014, 50).

Those who focus on internal limitations find two reasons why the United States cannot draft this type of doctrine. The first is that the nation's political and military leadership is unable to make the transition to a COIN strategy that is

enabled and prosecuted through cyberspace effects because they apply the thinking and analogies of previous generations of warfare (Betz and Stephens 2013, 148). Examples of this mindset include advisors like Haddick, who argues for pre-emptive OCO against foreign servers that threaten the United States because “deterrence and retaliation doesn’t seem the right model for cyber war” (Haddick 2010, 14). The other reason cited for this limitation is organizational; the retention of authority to conduct cyberspace operations at high levels of command creates a situation in which “the COCOM cannot plan and execute its own cyber effects” (Stallone 2009, 14).

While there are arguments like these against the United States’ ability to construct better doctrinal guidance, there are many more works that assume it is possible and describe what this guidance would look like. Some authors have approached this issue of describing how cyberspace operations can be conducted in a COIN by focusing on specific cyberspace actions or specific COIN tenets, though the descriptive words used in these articles vary. There are also works that attempt to map individual or multiple cyberspace actions against COIN tenets, but these works only address some of the cyberspace actions or COIN tenets.

2. Works that Provide Guidance on Cyberspace Operations’ Contribution to One or Two COIN Tenets

The largest body of work that argues for incorporating cyberspace actions and effects into COINs is that which is focused on a specific tenet of COIN or two, and how cyberspace operations can contribute to that tenet. As with the body of knowledge that doubts the applicability of cyberspace effects and actions in a COIN, there are some works in this group focused on the nature of the conflict and others focused on the United States’ internal limitations.

Temaat and Webster address the nature of the conflict by focusing on conducting cyberspace operations with effects which impact the information arena, from understanding the operational environment and sharing this

information with host nation (HN) and coalition partners (Webster 2010, 4-21), to disseminating the COIN commander's narrative to the population (Temaat 2006, 4). Brickley, Warren, and even Liles also address the nature of the conflict by focusing on how cyberspace defense can support securing the population by preventing cyber terrorism (Brickley 2012, 4–5, and Liles 2010, 51), and on how cyberspace operational preparation of the environment (OPE) can support the primacy of politics by disseminating HN political messaging (Warren 2011, 13).

Stallone, Vacca, and Schraeder all address internal United States limitations, with a strong focus on how the authority to conduct cyberspace operations should be delegated to COIN commanders. Stallone argues that a Joint Force Cyber Component Commander should be given control of all cyberspace operations in a given Theater of Operations (Stallone 2009, 14–17), while Vacca and Schraeder argue against this arrangement either because the nature of the threats we face makes a monolithic defense structure unwise (Vacca 2011, 170–171), or because a single commander would have cultural limitations stemming from that commander's branch affiliation (Schraeder 2008, 46–47). While these authors disagree on the form that the authority to conduct cyberspace operations should take, they all pursue an ideal command relationship because they recognize the role that cyberspace operations can play in ensuring unity of command, unity of effort, and synchronizing lines of effort (LOEs) and lines of operations (LOOs).

Other works regularly appear that address the application of cyberspace actions and effects to specific COIN tenets, but they often contain too few specifics on how cyberspace effects should be achieved, other than to say that they should be. Ringdahl provides a good example of this type of work as he recognizes that cyberspace operations can play a role in understanding the operational environment (OE), primacy of politics, and collecting the intelligence that can drive operations, though he provides little specific or even generalized examples of what this would look like (Ringdahl 2010, 7). Fidier takes a step in the direction of providing a framework for incorporating CO into COIN with his

mapping of cyberspace actions against the three fundamental operations of "Clear, Hold, and Build." Unfortunately, he provides few examples of what this would look like, and uses a mapping that does not align with the tenets of COIN (Fidier 2015). Fidier's approach also suffers from focusing exclusively on operations, ignoring the organizational benefits that cyberspace operations can provide.

3. Works that Provide Guidance on One or Two Cyberspace Operations' Contribution to COIN in General

The other body of work that provides guidance on cyberspace operations' contributions to a COIN do so by exploring a specific cyberspace action or two, and how they can contribute to a COIN. These works rarely address a specific COIN tenet, and often do not link the new use or form of a cyberspace action to effects in the COIN fight.

The first group of works in this body is focused on specific cyberspace actions, but does not map these actions to specific COIN tenets. Tan writes about the expansion of cyberspace defense, including cyber deception, and how this can assist a COIN commander in isolating an insurgency by interfering with insurgents' ability to access foreign support or domestic audiences (Tan 2003, 23–24). His paper then explores the additional assistance that expanded cyberspace defense can provide in defending the population and friendly government infrastructure through obfuscation and misdirection (Tan 2003, 48–51). Pendall, Wilkes, and Robinson write about the manner in which cyberspace operations contribute to intelligence preparation of the battlefield (IPB). They argue for a restructuring that better collects and disseminates information by examining operations in Afghanistan. Their work addresses the effects that this restructuring would achieve in expanding authorities and raising the United States military's appreciation of cyberspace operations in a threat environment that is increasingly more connected to the Internet (Pendall, Wilkes, and Robinson 2013, 4–5), but do not give examples of what the new means or effects in a COIN would look like. Thomas addresses the manner in which cyberspace

IPB and OPE are conducted from an Information Operations (IO) perspective, but his discussion of the effects achieved are limited to conducting operations quicker and in a manner that better appreciates local cultures (Thomas 2006, 26–28).

The second group of analyses in this body is focused on specific cyberspace actions, and maps these actions to specific COIN tenets, but these works are often only focused on one or two of these mappings. A 2011 report by the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD-ATL) examines the ways in which cyberspace actions and effects are applied to COINs by describing the ways in which the United States does or should conduct cyberspace ISR in support of the tenet of understanding the OE (USD-ATL 2011, 40 & 52). Eidman and Greene provide a good example of cyberspace ISR and OPE mapping to the tenet of developing the COIN narrative by their exploration of the way that Syria used the Syrian Electronic Army as a proxy militia to aid them in agenda setting (Eidman and Greene 2014, 35–45). Mills explores the way that states can respond to insurgent uses of the Internet by creating pro-state video games and expanding cyberspace ISR and OPE to isolate the insurgency (which feeds into securing the population), aid host nations in understanding their operating environment (which feeds into primacy of politics), and collaborating with outside agencies (which feeds into unity of command and unity of effort) (Mills 2011, 159). In all of these works, there are good examples of how to map one or more cyberspace actions against one or more COIN tenet, but none of these papers addresses all cyberspace actions or all COIN tenets.

E. THESIS OUTLINE

The preceding review shows a clear need for a more complete effort to integrate cyberspace actions into COIN operations and doctrine. All prior efforts have either dismissed even the possibility of effective U.S. use of cyberspace effects for COIN purposes, or have dealt with only selected actions and COIN

tenets. Specifically, there are no studies or articles that address all of the cyberspace actions in JP 3–12(R) and all of the COIN tenets in JP 3–24.

The work presented here is intended to address the gap in doctrinal thinking by first outlining the breadth of current primary cyberspace and COIN doctrines, demonstrating that current doctrine only provides an intent-based mapping of cyberspace operations to the COIN environment as a whole. Our analysis starts with the effects-based framework of cyberspace actions provided by JP 3–12(R) and cross-references these actions with the tenets of COIN provided by JP 3–24 to produce a comprehensive matrix of potential cyberspace applications in COIN operations. We then evaluate the matrix to determine where current doctrine does not provide sufficient guidance on the ways in which cyberspace operations can achieve effects that contribute to accomplishment of the COIN tenets. We categorize and prioritize these matrix entries, and propose additions to doctrine to address the insufficiencies with the highest priority. Finally, we discuss the limitations of this mapping and identify areas for future research.

II. CURRENT STATE OF DOCTRINAL GUIDANCE

A. JOINT PUBLICATIONS

Major combat operations are conducted in the modern era by joint commands. When conducting planning operations within these commands, Joint Publications must be referenced and used as the authoritative source for planning. It is here that guidance for the application of cyberspace operations in COINs should lie, but the two controlling publications that address cyberspace operations and COINs do not provide sufficient guidance for doing so.

1. Joint Publication 3–12(R), Cyberspace Operations

Only one unclassified Joint Publication has been published on cyberspace operations, JP 3–12(R), and it does not address COINs or any other specific types of military campaigns. While there is a classified version of this publication, and there are other documents that provide guidance at this level, JP 3-12(R) is the primary source of unclassified guidance for the conduct of cyberspace operations, and is addressed as such by this thesis. The publication begins by outlining the DOD-wide scope and framework for incorporating cyber forces into the joint force. JP 3-12(R) contextualizes cyberspace operations (CO) by describing cyberspace using a three-layer model consisting of physical, logical, and cyber-persona layers (United States Joint Chiefs of Staff (USJCS) 2013a, I-2–I-4). It also provides detailed guidance on authorities, roles and responsibilities, legal considerations, and planning and coordination. Within this context, JP 3–12(R) provides guidance on how to incorporate CO into Joint Operations via three frameworks.

First the publication introduces a categorization of COs based on their intent: Offensive CO (OCO), Defensive CO (DCO), and Department of Defense information network (DODIN) operations. This section of the publication includes examples of specific effects and mission types for DCO and DODIN operations

(USCJS 2013a, II-2–II-3), but these examples are neither exhaustive, nor do they pertain specifically to COINs.

Second the publication introduces guidance for distinguishing cyberspace actions based on their desired effects. It states that while missions may be divided by intent, accomplishment of these missions "will require the employment of various capabilities to create specific effects in cyberspace" (USCJS 2013a, II-4). The four distinguishable cyberspace actions are Cyberspace Defense, Cyberspace intelligence, surveillance, and reconnaissance (ISR), Cyberspace OPE, and Cyberspace Attack.

Finally, the publication addresses the division of joint operations into the six basic groups: Command and Control (C2), intelligence, fires, movement and maneuver, protection, and sustainment. It provides general guidance for incorporating cyberspace operations into these groups with "an overview of how each of these functions applies to effective joint operations in and through cyberspace" (USJCS 2013a, II-6). The bulk of this section is focused on authorities, integration, and deconfliction of cyberspace assets, but there is repeated mention of incorporating CO in a manner that achieves the Joint Force Commander (JFC)'s effects. The word "effect" or "effects" is used 16 times in these six pages, and the importance of weighing operational effects is illustrated well on page II-10 when the publication states that "CO capabilities, though they may be used in a stand-alone context, are generally most effective when integrated with other capabilities to create the JFC's desired effects."

The absence of guidance on COINs in JP 3–12(R) is understandable, as the goal of the publication is not to provide guidance for incorporating cyberspace operations into specific campaigns like COINs. The publication acknowledges this fact, and accounts for it by providing general guidance on incorporating CO into joint operations, and categorizes COs based on either their intent or effects for incorporation into any campaign.

Two observations may be made about JP 3-12(R). First, 33 pages of the publication are focused on the introduction and the DOD-wide framework and context, while only 12 pages are focused on the conduct of COs. This results in JP 3–12(R) providing more guidance on the administrative process of integrating cyberspace assets and operations into the joint force than on the ways in which cyberspace operations can achieve or support a commander's desired objectives. Second, the glossary notes that the terminology updated in JP 1–02 is the OCO, DCO, and DODIN categorization, and not the cyberspace actions. This gives the impression that the former framework is that which is most useful for assignment of forces and gaining authority to conduct CO, while the cyberspace actions form the framework that is most useful for incorporating CO into JO and other specific mission sets.

2. Joint Publication 3–24, Counterinsurgency

Given the lack of guidance provided by JP 3–12(R) on how to integrate CO into COINs, another place to look for this guidance in joint doctrine is the publication on COINs, JP 3–24. Joint publications on COIN from before this century did not address cyberspace directly, as it was not as well formed a discipline or war-fighting domain as it is now. The DOD has published two updated COIN publications in recent years, in October 2009 and November 2013. While the latest edition of this publication includes more discussion of CO than any other joint operations (JO)-specific or mission-set specific joint publication, it is the location within joint doctrine where the bulk of guidance on how to incorporate CO into COIN is provided. As a result, JP 3–24 deserves the most attention of cyberspace planners and operators who are assigned this mission.

The first two chapters in the body of JP 3–24 describe an insurgency and present the fundamentals of a COIN, including the tenets of COIN. The next three chapters outline the operational environment in which a COIN is conducted, and provide general guidance for how a COIN should be planned and assessed.

The last two chapters describe the role of supporting operations in a COIN, where cyberspace consideration are addressed, and address the governance issues relevant to conducting a COIN. While this framework does address cyberspace operations, there are three deficiencies in the publication for readers seeking guidance on how to support the tenets of COIN with the effects of cyberspace operations.

The first deficiency is the manner in which JP 3–24 presents the tenets of COIN. An initial, though relatively minor concern is the fact that the executive summary states that there are four tenets of COIN, but the body of the text discusses six tenets of COIN in detail. Where the publication discusses the tenets in detail, it presents the tenets of COIN as “guideposts for the joint force” (USJCS 2013b, III-7), and discusses details of missions ranging from roadblocks to Department of Treasury task forces, but does not link the tenets to cyberspace operations in any way. The text of the tenets which follows does not include the word cyber, and the two places where CO are discussed in any detail only make reference to two tenets: Understanding the operational environment (OE), which directly addresses CO, and defend the population, which indirectly addresses CO through acknowledging that CO can isolate the insurgency.

The second deficiency is in the generalized guidance that JP 3–24 provides for conducting CO in a COIN. The sole paragraph that provides this guidance only lists three missions for CO: isolating and separating the insurgency, denying the enemy freedom of action, and maintaining U.S. and joint forces freedom of maneuver (USJCS 2013b, VII-1). By comparison, the guidance on air operations covers four pages, addresses a wide array of operations, and provides detailed guidance on the conduct of many of these operations. Three portions of this publication make the limited attention paid to cyberspace operations more striking. First, the cyberspace operations paragraph outlines a wider array of mission sets that insurgents may be conducting. While this usefully highlights the types of enemy missions that CO can disrupt, it also suggests that more guidance can be provided on the mission types that friendly forces can

conduct. Second, specific guidance for different mission sets is provided for other support activities. One example is the discussion of air support, which includes granularity down to the level of specific air support mission sets and the aircraft frames appropriate for these missions (USJCS 2013b, VII-2–VII-5). Finally, appendix D includes a list of tactical and operations precepts that complement the generalized guidance for almost every other form of supporting activity but does not address cyberspace operations in any way.

The third deficiency is in presenting only an intent-based categorization of CO and not addressing the effects-based categorization of CO. As discussed, JP 3–12(R) provides the effects-based categorization for the purposes of linking CO to a JFC's desired effects, but JP 3-24 neglects to use this categorization. By comparison, the section on space operations mentions specific effects and links them to COIN tenets. If the cyberspace section were robust, and described how the effects of these three mission types were to be achieved, or how these three mission types complimented the COIN tenets, it may have provided better guidance. It not only fails to provide this guidance, but also provides a categorization of operations that has notable gaps and contradictions:

1. The definition of OCO provided in JP 3–24 restricts the conditions under which operations may be conducted against an insurgency by stating that they can only be conducted in response to a limited number of insurgent uses of cyberspace. Specifically, it does not call for OCO to be conducted in response to insurgent use of cyberspace to distribute training materials or other similar information. If planners relied solely on this publication for guidance, they would be precluded from executing missions like the unattributed actions that replaced the bomb-making instructions on a terrorist website with a recipe for making cupcakes (Spy Blog, 2011).

2. The definition of DCO that JP 3–24 expands the realm of cyberspace in which the military may conduct defensive operations to include host nation (HN) cyberspace, but provides limiting and seemingly contradictory guidance on the types of operations that may be conducted there. First, it limits

DCO to detecting and responding to adversary actions, with no mention of proactively hardening systems to withstand adversary actions. While JP 2-13(R) addresses this limitation by splitting DCO into internal and external missions, JP 3-24 does not. This gap indicates that all DCO will be reflexive or responsive. Second, the definition then states that these DCO would identify insurgents and create conditions for defeating them, which implies that DCO encompasses all intelligence gathering and battlefield preparation operations, including those that would be traditionally classified as intelligence operations of a decidedly offensive nature. This contradiction blurs the lines between JP 3–12(R)'s OCO and DCO definitions.

3. The definition of DODIN operations is replaced with a definition of "Building HN Cyberspace Capability" (USJCS 2013b, VII-2). The publication does not discuss DODIN operations at all, but provides a subparagraph in its place that frames this HN support as the DODIN-equivalent mission in a COIN. This definition is again limited in its scope, as it focuses only on strengthening those portions of HN cyberspace that are part of or at least loosely affiliated with the HN government, with no mention of the HN's civilian sector. This gap ignores the growing trend in building cyberspace capacity, as the growing trend in expanding cyberspace capability has been providing standards compliance training and infrastructure funding in both Europe (North Atlantic Treaty Organization (NATO) Industry Cyber Partnership) and the Middle East (National Institute of Standards and Technology–Middle East North Africa).

The result of these oversights, contradictions, and gaps is that JP 3–24 provides little specific guidance on how CO can produce effects that support a COIN. JP 3–24 informs the joint force that "[w]arfare that has the population as its focus of operations requires a different mindset and different capabilities than warfare that focuses on defeating an adversary militarily" (USJCS 2013b, ix). It also discusses the importance of the information environment in winning a COIN, and acknowledges the role that cyberspace operations can play. It does not,

however, give any guidance to the joint force regarding what these missions look like, or what effects they might achieve.

B. BRANCH-SPECIFIC DOCTRINE

The net effect of so little mention in doctrine of CO related to the tenets of COIN, is that the means with which CO can help achieve COIN ends are not sufficiently discussed. In the absence of joint doctrine that discusses the means of achieving effects, service publications often provide this information for their respective operators.

The Air Force Doctrine Document, 3–12, Cyberspace Operations, does provide limited additional guidance in this respect. The document not only relates cyberspace operations to the principles of JO and the tenets of air power (Department of the Air Force, 16–19); it provides examples of these relationships that include COIN or COIN-like operations conducted by and against the United States and its allies. This document does not address COIN tenets directly, and it includes some service-specific guidance that may not work well in a joint operation, the most notable example of which is the assignment of measuring tactical Measures of Performance (MOPs) and Measures of Effectiveness (MOEs) to air-domain ISR assets (Department of the Air Force, 32). While this document does not perform a mapping between cyberspace operations and the COIN tenets, it offers a vision for how such a mapping may be accomplished.

Outside of the Air Force's doctrine, the services provide no additional help in mapping cyberspace operations to the COIN tenets. The Army's doctrine on cyberspace operations, Field Manual (FM) 3–38, Cyber Electromagnetic Activities, expands on joint doctrine's definitions of the layers of cyberspace (physical, logical, and cyber-persona) and the authorities under which cyberspace operations are conducted, but it does not provide any insights into effects-based categorization of cyberspace operations. Instead, it repeats the process of dividing cyberspace operations into OCO, DCO, and DODIN operations. The FM then describes electromagnetic attacks, including examples

of the means with which these operations may achieve their ends. The same deficiency identified above in JP 3–24 is present in FM 3–38: examples of how to achieve effects are provided for all aspects of the publication's subject, except for cyberspace operations.

Providing less than the Army, the Marines' Marine Corps Order (MCO) 3100.4–Cyberspace Operations provides guidance for the manning, acquisition, and roles related to the Corps' cyberspace operations. The order provides some guidance on defense of their enterprise network, but neither the order nor any of its referenced documents contain guidance on the means of achieving cyberspace effects outside of this defensive role.

The Navy's equivalent document, Secretary of the Navy (SECNAV) Instruction 3052.2, Cyberspace Policy and Administration within the Department of the Navy, is similar to MCO 3100.4, but was written earlier so does not provide as much specific guidance and is not linked to the same Joint Publications. The Navy is addressing these and other concerns, as stated in U.S. Fleet Cyber Command/10th Navy's "Strategic Plan 2015–2020," by pushing for standardization in the methods of conducting and evaluating the success of cyberspace operations (Department of the Navy 2015, 17). This may yield insight on incorporating CO in COINs in the future, but provides little guidance for Naval personnel engaged in current COIN campaigns.

C. SHORTCOMINGS OF CURRENT DOCTRINE

The preceding review demonstrates the main limitations of current doctrine, rooted primarily in simply insufficient attention to articulating the full potential for applying cyberspace actions for COIN purposes. Joint doctrine only provides an intent-based mapping of cyberspace operations to COIN in a generalized sense. There is neither guidance on the types of cyberspace effects that support COIN tenets nor guidance on how these effects can be achieved. The guidance provided by individual branches varies by branch in the degree to which effects-based cyberspace operations can be planned, and none of the

branches connect cyberspace effects-based planning towards goals unique to their domains in a manner that applies to specific campaigns like COINs. The following chapter examines the effects that cyberspace operations can achieve in support of each the COIN tenets, and determines the degree to which current doctrine is insufficient in providing guidance on these effects and their contributions to a COIN campaign.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PROPOSED SOLUTION

This chapter introduces a matrix that maps cyberspace actions against COIN tenets. It describes the concept of this mapping, and how this mapping is used to evaluate the sufficiency of current doctrine. It explores this sufficiency with case examples when available, and determines how significant a contribution the effects described in each cell make towards accomplishment of COIN tenets. It concludes by introducing the general trends observed in conducting the mapping exercise that enable the cells to be categorized and prioritized.

A. THE MAPPING METHOD

The concept of mapping one list of items to another list, as applied here, enables focused attention on a detailed set of intersections of opportunities for cyberspace action and counterinsurgency needs. Specifically, this thesis maps the cyberspace actions identified in JP 3–12(R) to the COIN tenets identified in JP 3–24, as presented in Table 1. The cells at each intersection provide a description of the effects that the given cyberspace action may achieve in support of the given tenet.

The cyberspace actions utilized in this matrix are listed in JP 3–12(R), Cyberspace Operations. The complete descriptions of these actions are contained in Appendix A of this thesis, and are summarized as follows:

- Cyberspace Defense: “actions normally created within DOD cyberspace for securing, operating, and defending the DODIN.”
- Cyberspace ISR: actions “conducted to gather intelligence that may be required to support future operations, including OCO or DCO.”
- Cyberspace OPE: “non-intelligence actions conducted to plan and prepare for potential follow-on military operations.”
- Cyberspace Attack: “actions that create various direct denial effects (e.g., degrade, disrupt, and destroy) in cyberspace,” and includes the manipulation of adversary intelligence and information systems

that leads to denial in cyberspace or the physical domains (USCJS 2013a, 2013).

The tenets of COIN utilized in this matrix are listed in JP 3–24, Counterinsurgency. The complete descriptions of these tenets are contained in Appendix B of this thesis, and are summarized as follows:

- Understand the OE: providing a commander with sociocultural knowledge, an understanding of the United States' HN partners, preparation for a long-term commitment, U.S. public support, and the ability to learn and adapt.
- Develop the COIN Narrative: developing a narrative that contextualizes what the population experiences, legitimizes COIN activities, and delegitimizes the insurgency.
- Primacy of Politics: ensuring that U.S. government and HN political objectives guide the COIN approach.
- Secure the Population: providing human security, physical security, and rule of law by legitimizing the HN legal systems, mitigating unintended consequences of COIN operations, and isolating the insurgency.
- Synchronize and Integrate LOEs: integrating the efforts of joint interagency, multinational, and HN participants towards a common purpose.
- Unity of Command and Unity of Effort: providing unity between military forces and interagency partners, coordinating with NGOs, and enabling intelligence to drive operations (USCJS 2013b, 2013).

This chapter explores each of the intersections between the cyberspace actions and the COIN tenet. The order in which this thesis examines the cyberspace actions is different from the order in which they are listed in JP 3-12(R). This thesis examines them in the order in which cyberspace actions may be planned chronologically. It begins by examining the utility of cyberspace ISR, focusing on the way in which cyberspace operations can give a commander a view of the OE. It then examines the utility of cyberspace OPE, setting the conditions for both future cyberspace operations and achievement of the COIN tenets. It then examines the utility of cyberspace defense, exploring the contributions that it makes in defending US, HN, and other organization. It

concludes by examining the utility of cyberspace attack, focusing on the contributions it makes in isolating and defeating an insurgency.

Table 1. Mapping of Cyberspace Actions to COIN Tenets

		Cyberspace Actions			
		1. Cyberspace ISR	2. Cyberspace OPE	3. Cyberspace Defense	4. Cyberspace Attack
Tenets of COIN	a. Understand the OE	Evaluate HN Gov't Cyber Ability, Identify ISPs & Phone COs, Describe Civilian Pattern of Life	Develop Cyber Capability of HN Government and Civilian Sectors	Identify Critical Cyber Capabilities and Vulnerabilities within HN and Prepare Defenses	Preposition Physical Devices and/or Logical Backdoors in Relevant Systems
	b. Develop the COIN Narrative	Identify Popular Cyber Venues and Cultural Symbols used by Relevant Actors	Ensure Ability to Disseminate COIN Narrative Through Relevant Cyber Venues	[Not applicable]	[Not applicable]
	c. Primacy of Politics	Identify Challenges and Opportunities of HN Cyber Infrastructure	Strengthen HN Government Cyber Infrastructure Resilience, Train HN Cyber Forces	Defend HN Government from Cyberspace Attack	Deny Insurgents the Ability to Significantly Impact HN or Other Friendly Actors via Cyberspace
	d. Secure the Population	Identify Insurgent Logistical and Command and Control Channels	Distribute Friendly IO Messages and Counter Insurgent Messaging	Protect Friendly Critical Infrastructure, Collect Evidence from Thwarted Cyberspace Attacks	Isolate the Insurgency, Prevent Human & Physical Damage, Attack Insurgency Methods/ Resources
	e. Synchronize & Integrate LOEs	Synchronize & Deconflict CO with Relevant Actors, Especially Concerning Intelligence Gain/Loss (IGL)	Define COIN Commander's Cyber Sphere of Influence	Maintain Friendly Freedom of Movement Across the DODIN and HN Cyberspace	Synchronize & Deconflict CO with Relevant Actors, Especially Concerning Enabling Future Operations
	f. Unity of Command & Unity of Effort	Identify Cyber Activity and Communication Channels of Other Relevant Organizations	Maintain Friendly Freedom of Movement Across the Cyber Domain	Maintain Friendly Freedom of Movement Across the DODIN for All Appropriate Actors	Coordinate CO with Higher Echelons, Providing COIN Commander More Cyberspace Attack Options

Adapted from JP 3-12(R): Cyberspace Operations (Cyberspace Actions) and JP 3-24: Counterinsurgency (Tenets of COIN)

B. MATRIX CELL EXPLANATIONS AND CASE STUDY EXAMPLES

This section describes the mapping of each cyberspace action to the six COIN tenets, ordered first by cyberspace action and then by COIN tenet. Each examination begins with a general description of the effects that each type of cyberspace action can achieve in support of each COIN tenet. The examination then explores the degree to which current doctrine already provides this guidance. Current doctrine is considered excellent if it both describes the effects that cyberspace operations can achieve, and connects these effects with accomplishment of the COIN tenets. Current doctrine is considered sufficient if it either provides a description of the effects that cyberspace operations can achieve in general support of a COIN, or if it links cyberspace operations in general to specific COIN tenets. Next, the examination mentions whether case examples or proposed models for this type of operation already exist in open-source information. Finally, the examination explores the degree to which this type of operation contributes to a successful COIN campaign.

1. Cyberspace Action 1: Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR)

Cyberspace ISR collects and analyzes data from a broad range of sources. This thesis focuses on the specific effects that are listed in JP 3-12(R), and how they contribute to the accomplishment of each of the COIN tenets.

a. Mapping Cyberspace ISR to Understand the OE

Cyberspace ISR contributes to a commander's understanding of the Operational Environment by identifying the host nation's Internet service providers (ISPs) and phone companies, evaluating the host nation's cyberspace capabilities, and describing the civilian population's typical pattern of life.

Current doctrine provides limited guidance for the intersection of cyberspace ISR and understand the OE. JP 3–12(R) only discusses intelligence collection in a general sense, and does not connect intelligence gathering to the

OE. It abstracts this discussion away by referring to JP 3–13, Information Operations. JP 3–13 only discusses cyberspace operations in the context of a simple counting of information technology devices, and cyberspace operations' ability to influence an enemy's decision-making process. JP 3–24 acknowledges that the OE includes cyberspace components like "Internet communications such as e-mail and social networking sites" (USJCS 2013b, IV-3), but does not address the existence of cyber-unique characteristics of the civilian pattern of life. While the publication later states that "the joint force relies on cyberspace to develop a clear understanding of the OE" (USJCS 2013b, VII-1), the following discussion addresses this understanding only in the context of the insurgents' use of cyberspace technology. None of these publications address aspects of this appraisal that are unique to cyberspace, treating the Internet as a mirror of previous communication networks, like the telephone system. As a result, they all fail to include popular communication applications, cyber personas, and other cyber-unique elements that influence the OE.

There are no published reports of the cyber-specific intelligence that is gathered and reported to COIN commanders, likely owing to its classification. In open-source information, the intelligence community provides a generalized assessment of the communication networks for each nation, maintaining databases like the CIA's World Factbook (Central Intelligence Agency, 2013). When a COIN commander is assigned a nation or region, their cyberspace professionals may compliment this general communications intelligence with details about the region's cyber infrastructure. This additional intelligence addresses the population, the insurgency, and the host nation government. It addresses these groups by describing the physical devices, communication networks, applications, protocols, websites, and cyber personas that each group uses / accesses.

The degree to which the intersection of cyberspace ISR and understand the OE contributes to a COIN campaign is not significant. Current intelligence guidance and publically available records already account for much of this

information, but including these cyber-specific components helps to paint a more complete picture of the OE.

b. Mapping Cyberspace ISR to Develop the COIN Narrative

Cyberspace ISR helps craft the COIN narrative by locating the media that the insurgency uses to broadcast their narrative in cyberspace, in order to keep the command updated about the insurgent messages and responses to COIN operations. Cyberspace ISR also analyzes the media that the civilian population uses most often, in order to describe the lenses through which the population views the insurgency, HN, and COIN forces. This cyber-specific contribution entails analysis of the websites, blogs, and images that local IPSs cache the most often because they are regularly viewed or updated by either the population or insurgency.

Current doctrine does not provide guidance for the aspects of the intersection of cyberspace ISR and develop the COIN narrative that are unique to cyberspace. JP 3–12(R) does not address the COIN narrative. In the COIN narrative section of JP 3–24, it states that the COIN narrative "should invoke relevant cultural and historical references to both justify the actions of counterinsurgents and make the case that the government will win" (USJCS 2013b, II-9). It does not, however, follow this guidance with examples of what these references are or how to collect them. In the cyberspace considerations section of JP 3–24, it does not address the COIN narrative.

One example of a group conducting this type of operation is Hezbollah's use of Israeli national symbols in the cyberspace components of the Israeli-Palestinian conflict. By using these symbols on their website as part of their terrorist narrative, Hezbollah reflects "an 'us' and 'them' mentality, where Israelis and their American supporters, or else Palestinians and Muslims, are portrayed as barbaric, reflecting discourses of inclusion and exclusion" (Karatzogianni 2008, 6). Tapping into cultural symbols attaches a sense of inclusion between the host nation and its population without making such an attachment as overt as

calling for support. The United States often has permission to collect information that can tell which websites are most commonly accessed, and in some cases this information is advertised. Recording the symbols from those on-line sites and the personalities that they represent provides information operations professionals with a means to increase the public appeal of a COIN commander's narrative.

The degree to which the intersection of cyberspace ISR and develop the COIN narrative contributes to a COIN campaign is moderate. Cyberspace ISR of this sort provides the COIN commander with a quantifiable indicator that a cultural symbol or reference is popular. This does not guarantee that a reference is relevant, but it does contribute to the process of crafting a narrative that uses popular symbols. In addition, only cyberspace professionals can collect data across an entire nation in a matter of minutes to determine which symbols and references a specific audience is interacting with the most. The possibility of collecting this information for specific sections of the population, either geographically or along other lines, further enables a COIN narrative to appeal to its intended audience.

c. Mapping Cyberspace ISR to Primacy of Politics

Cyberspace ISR supports the Primacy of Politics by identifying the cyberspace challenges and opportunities that accomplishment of HN political goals faces. This involves collecting information about the cyber infrastructure of the HN that warrants the greatest amount of attention when conducting cyberspace OPE. Cyberspace ISR determines if a nation's civilian Internet service providers are conducting their business in a manner that makes it easier for insurgent groups to maintain their anonymity.

Current doctrine does not provide guidance for the intersection of cyberspace ISR and primacy of politics. JP 3–12(R) does not address HN cyber infrastructure. While JP 3–24 discusses building a HN's cyberspace capability, it does not state how that capability is measured before building or enhancing it.

Further, there are cases in which a focus only on the expansion of HN cyberspace capacity may do more to enable an insurgency than it does to legitimize a government.

One example is an ISP running “open resolver” DNS servers, because these allow insurgents to conduct both cache poisoning and low-level denial-of-service attacks with anonymity. Organizations like the Open Resolver Project simplify this process for cyberspace professionals, and present the importance of such practices in a manner that is easy for both COIN commanders and HN government officials to understand (Open Resolver Project, 2016).

Current doctrinal analysis frameworks referenced in JP 3-24, like ASCOPE (areas, structures, capabilities, organization, people, and events) and PMESII (political, military, economic, social, information, and infrastructure) (USCJS 2013b, IV-5), have not incorporated all of the information that can be collected about a HN’s cyberspace. For example, Cyberspace ISR can contribute to better measurement of a HN government’s defenses or cyberspace posture. Many scholars have presented matrices and metrics for measuring an agency or government’s resilience, but none have been formally integrated into analysis frameworks:

- Linkov et al. introduce a resilience matrix that determines a network’s resistance to attack. Their proposed matrix evaluates how each of the four domains of network-centric operations would react during the four life-cycle stages of resilient systems (Linkov et al 2013, 474).
- Mattern et al. build off of Lockheed Martin’s kill chain and present a proactive “course of action” matrix that can be used to measure progress in strengthening a government system (Mattern 2014, 709).
- Kieffer applies cyberspace IPB to network evaluation, arguing that basic network mapping and identification of key administrative accounts / personnel are useful measurements (Kieffer 2015, 12).

Cyberspace professionals can use tools like these to ascribe the HN a cyber resiliency measurement, and add this measurement to assessment frameworks like ASCOPE, PMESII, and DIME.

The degree to which the intersection of cyberspace ISR and primacy of politics contributes to a COIN campaign is moderate. It helps measure the progress of a HN government's development well, but only in this cyber-specific context. The Federal Bureau of Investigation (FBI) postulates that this type of evaluation provides a benefit in their efforts to strengthen HN rule of law. As a result, the FBI has developed a Cyber Assistant Legal Attaché (ALAT) system, which embeds legal professionals with foreign governments to "facilitate information sharing, increase cooperation on investigations, and improve relationships with foreign partners" (White House 2015). Cyberspace operators assigned to work with HN government cyberspace professionals can achieve similar benefits by gathering this information while they are providing the HN with security training (which is covered in the Cyberspace OPE portion of this thesis).

d. Mapping Cyberspace ISR to Secure the Population

Cyberspace ISR helps secure the population by identifying the means through which insurgents generate external financial and logistical support, and identifying the command and control channels that the insurgency uses. Information collected in cyberspace reveals insurgent channels of support both inside and outside of cyberspace. Examples of these types of operations include detecting and tracing online transactions through banks or cyber-unique currencies like Bitcoin, or detecting and tracing the distribution of information on the use and maintenance of equipment or weapons unique to the insurgency.

Current doctrine provides limited guidance for the intersection of cyberspace ISR and secure the population. JP 3–12(R) does not address securing a HN population. JP 3–24 states that DCO will detect enemy or adversary actions, though it does not say how. This publication also states that OCO will be considered if an insurgency uses cyberspace for a range of support

functions, but does not mention how these will be detected. JP 3–24 goes on to say that DCO will identify insurgent activities, though it is unclear how this will happen if DCO is limited to friendly networks, as outlined in the publication (USCJS 2013b, VII-21).

There are multiple case examples of this type of operation being conducted. As referenced earlier, an unknown organization (widely suspected to be the British intelligence agency) identified that insurgent forces were using the periodical “Inspire” to spread both their insurgent narrative and instructions on how to make improvised explosives (Flock 2011). Syrian hackers working in support of the Assad regime were able to identify the channels through which members of ISIS were communicating, and used this information to plant malware on an insurgent cell phone (Sanger and Schmitt 2015). United States forces can conduct similar operations to identify the channels over which insurgent groups are conducting both personal / internal communications, as well as the channel(s) through which they transmit their narrative and training information.

The degree to which the intersection of cyberspace ISR and secure the population contributes to a COIN campaign is significant. Cyberspace ISR supports this COIN tenet directly by providing a COIN commander the ability to target insurgent activity in cyberspace. Cyberspace ISR also supports this COIN tenet indirectly by generating intelligence about insurgent activity on the ground, which supports other operations that can help secure the population. Cyberspace ISR also may determine the types of weapon systems being used and other technical details about insurgent methods, giving ground forces a tactical information advantage in operations that secure the population and achieve other effects in support of a COIN.

e. Mapping Cyberspace ISR to Synchronize and Integrate LOEs

Cyberspace ISR synchronizes and deconflicts cyberspace operations with relevant actors, especially with regard to the intelligence gain / loss (IGL) that

may result from conducting cyberspace operations. Examples include weighing the benefits gained by denying insurgents the ability to communicate with specific devices or protocols or to access specific websites or people, against the benefits gained by collecting and analyzing this communications. While intelligence agencies provide expertise on the value of a specific source, cyberspace professionals provide the commander expertise about the integrity of data collected with different devices or means, and the risk of each type of collection being detected or compromised.

Current doctrine provides limited guidance for the intersection of cyberspace ISR and synchronize and integrate LOEs. JP 3–12(R) states that intelligence collection should be coordinated with other agencies and actors, but discusses the subject in no detail. JP 3–24 discusses intelligence issues but does not address the manner in which cyberspace intelligence collection operates in relation to other intelligence operations. JP 3–24 discusses information operations in great detail, and even discusses the concept of “compound strategies” (USJCS 2013b, II-13) but this section does not mention cyber. This publication’s cyberspace considerations section does not discuss the interaction that may occur between the cyber community and either the intelligence or information operations communities.

There is little public evidence of this type of operation being conducted. One example of a campaign not leveraging cyberspace assets to synchronize and integrate LOEs was the peacetime IO campaign in Bosnia. The IO and military information support operations (MISO) teams conducting operations in Bosnia were distributing messages that did not mesh well together and were occasionally counter-productive. While the IO and MISO communities eventually addressed these concerns by conducting a variety of meetings (Siegel 1998, 115), a cyber-led framework of storing and sharing messaging among coalition forces may have reduced these problems and the energy spent to mitigate them.

These operations also lacked substantial (MOEs), which led US forces to conduct operations that may or may not have been effective (Siegel 1998, 100–

101). Cyberspace ISR can prevent future instances of this deficiency by collecting information from popular websites, recording discussions of IO and MISO messages, and analyzing the frequency and character of these discussions through means including simple word count and associated favorable or unfavorable key words.

The degree to which the intersection of cyberspace ISR and synchronize and integrate LOEs contributes to a COIN campaign depends on the scope of the campaign, but rises to a moderate degree of significance at best. Larger campaigns will have more actors whose actions will benefit from cooperation and a greater amount of useful feedback, but they will have other means of providing coordination and measuring performance or effectiveness.

f. Mapping Cyberspace ISR to Unity of Command and Unity of Effort

Cyberspace ISR provides information for the commander about the cyberspace activity of other military forces, government organizations, and affiliated international organizations that may help or hinder the commander's goals. Cyberspace ISR also identifies the different communication channels that these and other organizations use to transmit or receive information over the Internet, so that message distribution is not hindered by unidentified incompatibilities between different cyberspace actors.

Current doctrine provides limited guidance on the intersection of cyberspace ISR and unity of command and unity of effort. JP 3–12(R) states that intelligence collection should be coordinated with other agencies and actors, but discusses the subject in no detail. JP 3–24 provides mixed guidance on this cell. Where JP 3–24 succeeds is in addressing the second and third order effects of cyberspace operations (USJCS 2013b, VII-1), which is a minimal mention of this cell. Where JP 3–24 fails is that it addresses the importance of other agencies and organizations within an OE, but does not indicate that they will use the Internet or that this component of their involvement in the OE should be

addressed. By comparison, the maritime considerations section of JP 3-24 includes other organizations' use of the ocean, and provides specific guidance on "establishment or expansion of maritime domain awareness efforts" (USJCS 2013b, VII-7).

There is a model for this intersection. The Air Force has established a command that is focused on merging ISR and cyberspace operations. The model that they present is to divide cyberspace ISR into ISR collected *for* cyberspace operations, and ISR collected *by* cyberspace operations. This shift in organization would better align cyberspace efforts with intelligence capabilities than the present command relationship in which cyberspace operations fall under Information Operations by involving them more in the intelligence cycle that is identified as a subcomponent of this COIN tenet (USJCS 2013b, III-15). Cyberspace professionals can suggest Priority Information Requests (PIRs) to enter into the COIN intelligence planning process that perform the two functions that the Air Force identified (e.g., collection of intelligence for and by cyberspace operations).

The degree to which the intersection of cyberspace ISR and unity of command and unity of effort contributes to a COIN campaign is moderate. In cases where insurgent activity is detected in both cyberspace and physical dimensions, this is only a contributing or confirming source of intelligence. In cases where insurgent activity is revealed only through on-line activity, well-crafted priority information requests (PIRs) may give a COIN commander valuable insight or warning based on indicators that cannot be measured in any other domain.

2. Cyberspace Action 2: Cyberspace Operational Preparation of the Environment (OPE):

Cyberspace OPE often builds on the information collected by cyberspace ISR, and offers unique contributions in a COIN. This thesis explores these

contributions, and focuses on their contribution to the accomplishment of each of the COIN tenets.

a. Mapping Cyberspace OPE to Understand the OE

Cyberspace OPE includes measuring and expanding existing Internet capability in the host nation, and ensuring that all relevant stakeholders in the nation's Internet infrastructure and government are connected to the COIN effort. Examples include the establishment or strengthening of the host nation government's cyberspace forces, ISPs, and phone companies; ensuring that these groups follow as many internationally accepted best practices as possible; and ensuring that these groups are trained to recognize and report possible illegal / insurgent activity.

Current doctrine does not provide guidance for the intersection of cyberspace OPE and understand the OE. JP 3–12(R) does not address stakeholders in a contested OE. JP 3–24 discusses the importance of non-state actors within the OE, but does not discuss ways in which US forces can engage with them in a cyberspace context.

There have already been examples of this type of preparation in the Middle East. The National Institute of Standards and Technology (NIST) and the Jordan Institute for Standards and Metrology (JISM) held a conference in 2010 that addressed the infrastructure of the Middle East / North African (MENA), and its compliance with a range of standards (National Institute of Standards and Technology 2010). This conference was focused on a wide range of standards, and has not been repeated in the region. While compelling another agency to conduct international committees is outside of a COIN commander's authority, applying a similar strategy to meet with the government and industry leaders of a host nation is possible. Cyberspace professionals can also work with contracting professionals in the commander's staff to include NIST standards as a requirement for the infrastructure development that the DOD provides, and can work with other agencies to encourage them to take similar steps.

The degree to which the intersection of cyberspace OPE and understand the OE contributes to a COIN campaign is significant. Civilian cyberspace devices and networks that are properly configured limit the number of locally exploitable cyberspace assets that insurgents can use to channel information or conduct attacks. Local businesses that detect and report insurgent behavior in their networks or on their devices will help the COIN commander collect intelligence that is unavailable through non-cyber means. Further, ensuring that local businesses meet NIST and other international bodies' requirements for conducting business strengthens the economy and provides more legitimate opportunities for the local population to succeed. This helps reduce the number of disadvantaged members of the population who may support or join an insurgent organization.

b. Mapping Cyberspace OPE to Develop the COIN Narrative

Cyberspace OPE ensures that the government is able to disseminate its messaging directly to the public through the channels that they most often use. While these channels may vary by region or nation, once cyberspace professionals have identified the on-line arenas that are most popular with the HN population, they ensure that the HN government has access to these channels.

Current doctrine does not provide guidance for the intersection of cyberspace OPE and develop the COIN narrative. JP 3–12(R) does not address the COIN narrative or the conditions that would best enable a COIN commander or HN to transmit it. JP 3–24 focuses on the distribution of the COIN narrative when it states, "the compelling aspect of the narrative is not only in its content, but how it is presented (i.e., promoted and publicized) to the target audience, which normally requires ideological leaders (USJCS 2013b, II-4)." It does not, however, propose any aspects of transmitting this narrative other than the requirement that ideological leaders be involved.

One example of directing messaging through popular channels is the Yemeni Prime Minster's communications with the public through Facebook. Upon taking office, Prime Minister Khalid Mahfoud Bahah used Facebook to explain the reasoning and justification behind his decision to shuffle many cabinet members aside. He then solicited recommendations from the public for who should fill the vacancies in his cabinet. This direct engagement was hailed by many media observers in the country as a culturally sensitive move that appealed to the public, and it also gave the population a way to air their grievances (Al Batati 2014).

Cyberspace professionals are not required to recommend which types of communication and appeals the government expresses to the public, but they should ensure that the government is prepared to send these appeals to as wide an audience as possible. They accomplish this by ensuring that the HN is aware of these channels, and has an account ready to use to broadcast over these channels.

The degree to which the intersection of cyberspace OPE and develop the COIN narrative contributes to a COIN campaign is moderate. There are other means through which to convey a COIN narrative, but these types of operations give the HN government and COIN commander a means of conveying their narrative and other communications through the channels that are becoming increasingly popular and significant.

c. Mapping Cyberspace OPE to Primacy of Politics

Cyberspace OPE supports the primacy of politics by strengthening the portions of a host nation's government and nationwide cyber infrastructure that are vulnerable to attack. One way that these vulnerabilities are located and mitigated is through conducting DCO war games, in which friendly hackers identify weaknesses in the host nation's cyber infrastructure, and recommend changes that need to be made. These recommendations often include changes to network architecture, security procedures, and bandwidth/capacity.

Current doctrine does not provide guidance for the intersection of cyberspace OPE and primacy of politics. JP 3–12(R) does not address HN governments' political goals or legitimacy as a planning or operational consideration. JP 3–24 presents the view that understanding the OE in a COIN "poses a particular challenge for the JFC, as it is difficult to analyze one's own actions with the same objectivity as the JFC is able to apply to the decision making of others (USJCS 2013b, IV-12)." In cyberspace, these rules are less applicable, because these objectivity concerns are largely eliminated through the conduct of DCO exercises.

NATO is already conducting DCO exercises like these on an annual basis. Named "Operation Locked Shields," this exercise continues to increase the sophistication of the simulated attacks and the number of participating nations (North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence 2014). When a COIN commander is ordered to assist a nation that does not participate in exercises like these, they should include the host nation in existing exercises or develop new exercises.

One potential source of information on which to base these exercises is the Department of Homeland Security (DHS) guide for evaluating system vulnerabilities, which was recently praised by the Office of the Inspector General (OIG) (Office of the Inspector General 2014). The utility of the DHS' system has been addressed in by Sandia Laboratories (Mateski et al 2012), and similar vulnerability assessments are referenced in academic papers measuring operational levels of cyber intelligence (Mattern et al 2014, 707–708, and 715–716). Between the DHS' well-reviewed guide and the equivalent assessments proposed, there are frameworks available for a commander to use in developing a white-hat exercise if the supported HN government is unable or unwilling to work with NATO.

The degree to which the intersection of cyberspace OPE and primacy of politics contributes to a COIN campaign is moderate. If an insurgency is able to deface HN government websites or transmit false messages with compromised

HN social media accounts, they may weaken the HN government's perceived legitimacy. Helping a HN to enhance the security of their cyberspace infrastructure can prevent or mitigate these effects.

d. Mapping Cyberspace OPE to Secure the Population

Cyberspace OPE helps to secure the population by distributing friendly IO messages and countering insurgent messaging. Proactive examples of this include sending text messages or emails to specific populations that help support the legitimacy of the host nation government or that provide behavioral changes that will make insurgent activity easier to detect. Reactive examples of this include responding to inaccurate or misleading insurgent messages.

Current doctrine provides limited guidance for the intersection of cyberspace OPE and secure the population. JP 3–12(R) does not address the manner by which cyberspace professionals prepare a commander for messaging campaigns. JP 3–24 includes a section in which it "Describe[s] the Impact of the Operational Environment on Adversary and Friendly Capabilities (USJCS 2013b, IV-12–IV-15)," but it only provides a list of insurgent uses of cyberspace and the effects they can achieve. It does not give a similar list for what a COIN commander can do or achieve.

One example of proactive communications is the publically declared methods under which the HN will accept the surrender of insurgent forces. India faces various insurgencies in its northeast territories, and has publically posted its surrender policy on the Internet (Government of India). Many groups have surrendered themselves to the government under these clearly stated terms. The Aceh government has communicated directly with some of the insurgents it has faced, and this direct offer of a negotiated surrender has worked to bring in the country's most wanted insurgent leader (Simanjuntak 2015). Cyberspace professionals distribute the messages that the HN and COIN commanders prepare and ensure that they are distributed over the channels that are most often viewed by target portions of the population or insurgency.

One example of reactive communications is the counter-propaganda campaign of Malaysia in the 1980s. In that insurgency, British forces identified the channels that insurgents were using to broadcast their propaganda, and immediately responded to insurgent propaganda with their own messages. The Malaysian Communist Party (MCP) was pushed to invest significant resources countering this effort because the British enabled local Chinese and ex-MCP members to immediately respond to insurgent messages and to create their own (Ong 2010, 39–40). Cyberspace professionals have the opportunity to prepare the operational environment by identifying the forums where these conversations are already being had, and to help direct responsive messaging more effectively towards thwarting insurgent propaganda.

The degree to which the intersection of cyberspace OPE and secure the population contributes to a COIN campaign is significant. JP 3–24 recognizes the importance of enabling communication with insurgents by observing that “most insurgency solutions involve some sort of political compromise and are rarely a “winner take all” situation (USJCS 2013b, III-10–III-11).” This form of OPE enables compromise on an individual level; subverting individual members of an insurgency even when an insurgent organization is unwilling to compromise.

e. Mapping Cyberspace OPE to Synchronize & Integrate LOEs

Cyberspace OPE includes the process of defining which portions of cyberspace the commander can act in, and which actions they can conduct. This range of actions will stem from United States codes and laws, but will be modified by agreements with host and other nations, cooperation with other U.S. and third-party agencies, and the private companies acting within the host nation. Deconflicting responsibilities ahead of time in cyberspace may look similar to deconflicting fires in traditional joint operations, but it may also have unique aspects that make examples of this process difficult to identify.

Current doctrine provides extensive guidance for the intersection of cyberspace OPE and synchronize and integrate LOEs. JP 3–12(R) contains

extensive guidance for Cyber Support Elements (CSEs), and how they should coordinate their efforts with other government agencies (USJCS 2013a, III-6). JP 3–24 does not expand on this guidance to state whether there are any additional requirements in a COIN environment, and the OE of each COIN can vary widely enough that this omission appears wise.

Cyber teams that are assigned to COIN campaigns integrate their efforts with the rest of the fight through different liaisons and efforts. One proven model for how this integration is to include a cyberspace professional in COIN fusion cells, based on the way in which this has worked for Special Operations Forces (SOF) in Iraq and Afghanistan (Dinerman 2015). This SOF model has been suggested as a model for cyber teams to use in integrating their operations with COIN LOEs because of similarities between these two types of warriors—their methods are not well understood by conventional forces, they operate out of separated bases or parts of bases, and they work in a more covert manner than other forces (Dinerman 2015). Cyberspace operators who have representatives in a fusion cell coordinate their efforts with other parts of the COIN force to contribute more of the nation's cyberspace resources to a COIN campaign.

While current doctrine provides extensive guidance for the intersection of cyberspace OPE and synchronize and integrate LOEs, the contribution of this cell to a COIN campaign is minimal. The importance of linking operations and objectives as suggested in this cell is vital, but that is an understood component of military operations in general. The contribution of formalizing the guidance identified by this cell would be to formalize and give permanence to this type of coordination.

f. Mapping Cyberspace OPE to Unity of Command and Unity of Effort

Cyberspace OPE supports a commander by ensuring that friendly forces are able to maintain freedom of movement across the cyberspace domain. Examples of this include gaining permission to use private cyber infrastructure

within the host nation, and identifying routes that data must travel to avoid nations that do not grant the United States the cyberspace equivalent of “fly over” rights in cyberspace communications between the host nation and the United States.

Current doctrine provides minimal guidance for the intersection of cyberspace OPE and unity of command and unity of effort. JP 3-12(R) states that cyberspace operations require unity of effort, but it only describes how unity of effort can be achieved can be achieved for centralized missions like global defense. The publication states that any further command and control of cyberspace forces will be outlined in the concept of operations (CONOPS) and operation orders (OPORDS) published by a JFC (USJCS 2013a, II-6-II-7). JP 3-24 does not provide guidance on the preparation of cyberspace for conducting COIN operations. While there is guidance that this coordination *will* occur, it has come so recently that doctrine has not provided guidance for *how* this will occur.

The Secretary of Defense has mandated inclusion of cyberspace operations into Unity of Command and Unity of Effort. The new cyberspace model approved in June 2013 by the Secretary of Defense is a “Direct Support” C2 model that provides direct support to combatant commanders through four service-specific Joint Force Headquarters-Cyber (JFHQ-C), and also has classified components (Department of Defense 2014, 10). Given the military-specific nature of this model, it is likely designed to address a COIN commander’s concerns related to coordination with only U.S. and other allied forces. This model may also either address coordination with NGOs and inclusion of cyberspace operations in the intelligence-driven operations process, or provide a model for what that coordination looks like.

The degree to which the intersection of cyberspace OPE and unity of command and unity of effort contributes to a COIN campaign is significant. Gaining the authority to use other nation’s cyberspace in a “flyover” capacity prevents or mitigates international disagreement. Gaining the authority to work with local, private cyberspace actors expands the scope of cyberspace

professionals' ability to collect intelligence and ensures that best practices are being conducted. Both intelligence and best practices have been mentioned earlier—proper coordination not only enables planned COIN operations, but opens channels for local, private input that may yield additional opportunities.

3. Cyberspace Action 3: Cyberspace Defense

Cyberspace defense can begin without any OPE, but may be more effective if cyberspace ISR and OPE have been conducted. This thesis explores the range of effects that cyberspace defense can achieve in a COIN, and focuses on their contribution to the accomplishment of each of the COIN tenets.

a. Mapping Cyberspace Defense to Understand the OE

Commanders expect to know the vulnerabilities of friendly military bases and critical infrastructure, and that there are plans in place to defend these sites if they are attacked. Cyberspace Defense provides equivalent information and planning in cyberspace by identifying the critical cyberspace capabilities and vulnerabilities of both civilian infrastructure and government systems within a host nation, and preparing defenses of these systems in case of attack.

Current doctrine provides limited guidance for the intersection of cyberspace defense and understand the OE. Both Joint Publications avoid discussion of cyberspace actions in privately owned cyberspace. While there are limits on the military's ability to act in United States citizens' privately owned cyberspace, there are precedents for civilian actors pursuing government intervention, but there is no doctrinal answer for the means by which a COIN commander would respond to such requests.

Previously mentioned efforts like Operation Locked Shields help a HN to identify the vulnerabilities that it has in some of its infrastructure and most of its government-run systems. One example of addressing identified weaknesses was the Polish cyberspace defense effort in the wake of hacking incidents against Estonia, Ukraine, and the Polish energy infrastructure (van Blommestein 2014,

1). Poland refined its internal legal definitions, published security guidelines for public administration users, joined NATO's CCDCOE, incentivized Polish universities to develop new cryptography systems, and introduced a new phone security system (van Blommestein 2014, 2–5). Cyberspace defense supports COIN by identifying which systems are vulnerable, and addressing these weaknesses with as many measures as possible. While a supported HN may not be able to join a NATO team or possess a university system capable of developing new cryptography system, a partial or equivalent set of measures provides a COIN commander with a picture of a nation's weaknesses and the efforts taken to address them.

The degree to which the intersection of cyberspace defense and understand the OE contributes to a COIN campaign is significant. In addition to any benefit that local, private cyberspace actors may receive and render from interactions planned by a COIN commander, this type of interaction opens the door to American businesses' best practices being shared with private businesses within a COIN OE. If local businesses adopt new security protocols and encryption standards as a result of engagement, they will connect their new capabilities with the COIN effort, which may make them more receptive to other coordination and support activities in the future.

b. Mapping Cyberspace Defense to Develop the COIN Narrative

This intersection is not addressed because there is no logical way to map this cyberspace action to this COIN tenet. There is no portion of the HN government, civilian cyberspace infrastructure, or the DODIN that is used to develop or disseminate the COIN narrative that is not already accounted for in the mapping of cyberspace defense to other COIN tenets. While the successful defense of these networks against attack may validate the COIN narrative, it does not contribute to its development.

c. Mapping Cyberspace Defense to Primacy of Politics

U.S. cyberspace operators assess the likely threats posed to the DODIN and HN by the enemy. They execute operations that defend the DODIN and HN either through local means, or in coordination with the strategic teams assigned to defend the DODIN at the national level.

Current doctrine provides sufficient guidance for the intersection of cyberspace defense and primacy of politics. JP 3–24 provides guidance that DCO are conducted to defend friendly networks, which can be reasonably assumed to include all government cyberspace activity. It then links these effects this to primacy politics by stating that DCO will protect HN governance and sovereignty.

One recent example of cyberspace defense operations that supported the primary of politics was the Ukrainian defense of their election results system in 2014. This election was a critical event in maintaining the legitimacy of the Ukrainian government in the wake of the relatively new Russian-backed insurgency in with Eastern provinces. Approximately 72 hours before the election the hacker group CyberBerkut attacked the election results distribution system, destroying software, hardware, router settings, and even the system's main backup (Coker and Sonne 2015, 1–2). Ukrainian cyberspace defenders responded to the attack and were able to both repair the damage done and strengthen the system against future attacks. While there were still some attacks that day, including a distributed denial-of-service (DDOS) attack that did no damage and a DNS spoofing attack that was quickly remedied, the election results were distributed nation-wide, and the potential damage was minimized (Coker and Sonne 2015, 6–7).

The degree to which the intersection of cyberspace defense and primacy of politics contributes to a COIN campaign is significant. The actions in Ukraine provide a perfect example of a case in which no portion of national power except

cyberspace operations could defend against an attack that threatened to weaken both a nation's political system and its legitimacy.

d. Mapping Cyberspace Defense to Secure the Population

Cyberspace defense operations do not provide human and physical security directly, instead securing the population indirectly by isolating the insurgency, protecting friendly cyberspace capabilities, and mitigating cyberspace vulnerabilities in all layers of cyberspace. These operations reduce the number of networks that can be manipulated to aid malicious cyberspace activity, and collect forensic evidence that helps identify the source of insurgent malicious activity.

Current doctrine provides extensive guidance for the intersection of cyberspace defense and secure the population. JP 3–24 address the importance of this type of operation, with special notice paid to the importance of stopping insurgent criminal activity in cyberspace. This cell represents one of the few cases in which doctrine provides examples not only of how insurgents use cyberspace to achieve their objectives, but also how this creates possibilities for cyberspace professionals to contribute to COIN campaigns.

One example of cyberspace defense securing the population is the international response to Ukraine's insurgency. This response includes funding and training towards bolstering the cyberspace defenses of Ukraine's civilian sector. Romania spearheads these efforts, providing the bulk of the money and technical expertise provided to Ukraine through the Ukraine Cyber Defense Trust Fund (Fiscutean 2015). Romania provides an excellent model for providing cyberspace defenses specifically geared towards the COIN tenet of securing the population for two reasons. First, they support the safety of the population directly through their innovative "Bitdefender Box," which is made specifically for home networks (Mutler 2015). Second, they provide support to strengthening the rule of law through the work of their cyber-savvy police force's contribution to Europol efforts in the nation (Mutler 2015).

The United States also possesses significant cyberspace defense expertise in its public and private arenas, which it can apply and share with HN partners in a COIN. The Department of Homeland Security has consolidated the largest portion of the nation's defensive cyberspace resources under its Cyber Defense Initiative. In addition to this initiative, the Department of Defense recently reorganized its DODIN operations under a Joint Task Force (JTF)-DODIN. The JTF-DODIN has expanded its capabilities by incorporating and combining resources from the Defense Information Systems Agency (DISA), cyber command, and other military services (Miller). Between the expanded capabilities of the JTF-DODIN and the workshops and other resources from the DHS' CDI, US cyberspace professionals have many resources to apply in securing the population and strengthening the rule of law within a HN.

The degree to which the intersection of cyberspace defense and secure the population contributes to a COIN campaign is significant. Preventing an insurgency from exploiting local cyberspace actors is one of the core contributions that cyberspace professionals make in supporting a COIN campaign. Successful defense of local cyberspace actors both legitimizes the government and reinforces the COIN narrative, separating the insurgency from the local population.

e. Mapping Cyberspace Defense to Synchronize and Integrate LOEs

Cyberspace defense operations are conducted to ensure friendly freedom of movement across the DODIN and host nation cyberspace, so that all forces within the command can communicate freely with U.S. and host nation forces. Examples include identifying and securing vulnerabilities in communication software, identifying "bottlenecks" of limited bandwidth so that infrastructure projects are better prioritized, and standardizing protocols or developing translation algorithms to minimize compatibility issues between different systems' communication protocols.

Current doctrine provides sufficient guidance for the intersection of cyberspace defense and synchronize and integrate LOEs. JP 3–12(R) and JP 3–24 state that this is one of the core functions that cyber forces contribute to a supported commander. JP 3–24 also provides a brief description of how cyber crime negatively impacts the OE, which tells cyberspace defenders which activities they should prepare to thwart. The only failing of these publications is that neither one addresses the possibility of more sophisticated attacks coming from a COIN OE. This has not yet occurred, but it is a possibility which doctrine should address.

There are many examples of civilian companies reviewing the logs collected by other companies or by government agencies. Companies like Splunk provide Security Incident Event Monitoring to address the inability of local or small businesses to conduct thorough analysis of all logs. Splunk's terminology, taken from their corporate tag line is that they provide this service because "ninjas are too busy (Splunk 2016)." NIST guidelines for computer security log management echo this approach, advising that an organization prioritize log management appropriately throughout the organization by "establishing log management duties at both the individual system level and the log management infrastructure level (Kent and Souppaya 2006, ES-2)."

This division of labor is consistent with traditional military echelons of responsibility and can exist between a local COIN commander's cyber teams and the national cyber centers. In response to a new threat, the cyberspace team assigned to a commander prepares defenses and coordinates immediate response. Higher headquarters or echelons then provide assistance in log analysis and data correlation by comparing local threats against global trends and sharing lessons learned form local COINs with the rest of the DOD cyber community.

The degree to which the intersection of cyberspace defense and synchronize and integrate LOEs contributes to a COIN campaign is largely determined by the sophistication of the enemy, and there have been no case

examples where this analysis would have provided a significant contribution. In situations like the aforementioned CyberBerkut attack against Ukraine, the only challenge for cyberspace defenders is to generate an immediate response. More sophisticated attacks are not common, but when they occur, it is much easier to detect them and defend against them with the help of centralized log analysis element.

f. Mapping Cyberspace Defense to Unity of Command and Unity of Effort

Cyberspace operators support Unity of Command and Unity of Effort by maintaining friendly freedom of movement across the DODIN and between friendly forces, other government organizations (OGOs), and any relevant non-governmental organizations (NGOs). Examples include maintenance of friendly physical cyber architecture, continued access to venues for sharing information with relevant OGOs and NGOs, and publishing protocol standards for all friendly cyberspace communications.

Current doctrine provides minimal guidance for the intersection of cyberspace defense and unity of command and unity of effort. While both JP 3–12(R) and JP 3–24 address the freedom of action for US and allied forces, they do not speak to the freedom of action for unaffiliated actors. This may be due in part to an aversion to give guidance about military actions outside of United States Code authority, but as discussed earlier, there may be a request from private or outside, unaffiliated actors to provide this service.

This thesis has already mentioned the input from OGOs like openresolver.com, but there are many other OGOs, companies, and government agencies whose cyberspace security interests align with the DOD's. Cyberspace professionals tap into these different organizations when and if their help is needed and their interests align.

There are examples of this type of partnership in both addressing temporary issues and forming more permanent organizational alignments. A

recent example of corporate-government partnership in addressing insurgent operations is the cooperative investigation into ISIS' acquisition of vehicles, where the Department of Treasury and Toyota are working together to trace vehicle sales and transport (Luibrand 2015). A recent model of organizational partnership is the newly created National Background Investigations Bureau (NBIB). Under this model, the DOD provides the security and infrastructure around which the Office of Personnel Management (OPM)'s Federal Investigative Service (FIS) conducts and stores its investigations (Goldstein 2016).

The degree to which the intersection of cyberspace defense and unity of command and unity of effort contributes to a COIN campaign is moderate. While outside actors may fall victim to cyber crime, which aids an insurgency, local defensive measures will likely not prevent the majority of an insurgent group's cyber crime activity. There is some benefit from working with other agencies that share common goals, so that they can contribute to the COIN campaign without as much interruption by insurgent groups.

4. Cyberspace Action 4: Cyberspace Attack

Cyberspace attack includes the direct denial of insurgent uses of cyberspace, as well as the manipulation of insurgent cyber infrastructure. This thesis explores the range of effects that cyberspace attack can achieve in a COIN, and focuses on their contribution to the accomplishment of each of the COIN tenets.

a. Mapping Cyberspace Attack to Understand the OE

Cyberspace attack contributes to a commander's understanding of the OE by placing physical devices in key points of the physical layer of cyberspace in the target nation, or by placing logical capabilities on systems that are key points in either the physical or logical layer of cyberspace. Examples include packet sniffers that relay data to a centralized collection point, or accounts created by U.S. cyberspace actors that could both grant access to view data on specific systems and deliver effects via cyberspace in future operations.

Current doctrine provides no guidance for the intersection of cyberspace attack and understand the OE. The term that is used in a wide range of joint and service publications to describe devices like these is “sensors.” JP 3–12(R) only mentions sensors three times, and only does so to say that sensor data should be shared and relayed. JP 3–24 addresses sensors once, to say that they help build a common operating picture (COP). Given the library of doctrinal guidance on the placement and use of sensors across multiple domains, this lack of guidance on sensors in the cyber domain is striking.

There are open-source programs underway in the U.S. government, like Intelligence Advanced Research Projects Activity (IARPA)’s Cyber-attack Automated Unconventional Sensor Environment (CAUSE), which “aims to develop and test new automated methods that forecast and detect cyberspace attacks significantly earlier than existing methods” (Intelligence Advanced Research Projects Activity 2016). Determining where to place sensors or collect data is a process that is unique to each nation and threat, so these types of operations will be strongly connected to establishing the patterns of life of both groups to make anomalous behavior more obvious.

There are no instances of covert operations to collect data publically shared and acknowledged by the United States, but there are some examples of this behavior not being conducted. Insurgent groups like Boko Haram leave digital traces like everyone else, yet the African nations fighting them are not collecting even open-source forms of this data, to their detriment (Ajike 2015, 32). Whether or not the United States and its HN allies are repeating this mistake is not a matter of public record, though this type of data collection represents a cyberspace operation that can provide a COIN commander with a significant edge.

The degree to which the intersection of cyberspace attack and understand the OE contributes to a COIN campaign is significant. Just as ground sensors, imagery, and signals intelligence have collected information about impending

attacks in the past, cyberspace sensors provide a COIN commander with valuable warning about attacks in both the cyber and physical domains.

b. Mapping Cyberspace Attack to Develop the COIN Narrative

This intersection is not addressed because there is no logical way to map this cyberspace action to this COIN tenet. There is no component of drafting or delivering the COIN narratives of the HN or COIN commander that requires the denial or manipulation of adversary computer systems.

c. Mapping Cyberspace Attack to Primacy of Politics

Cyberspace attack supports the Primacy of Politics by denying insurgents the ability to significantly impact HN or other friendly actors via cyberspace. Examples include taking control of malicious botnets, deactivating or reconfiguring compromised components of cyberspace, or limiting insurgent freedom of movement over cyberspace by reconfiguring routers to ignore data from insurgent devices.

Current doctrine provides sufficient guidance for the intersection of cyberspace attack and primacy of politics, as it describes some effects that cyberspace attack can achieve, but does not connect these effects to the primacy of politics. JP 3–12(R) does not address a HN government's legitimacy or the HN population. JP 3–24 provides targets for OCO (insurgent resources, digital media, and "training, communication, and planning capabilities" (USJCS 2013b, VII-1), but it does not provide examples of the operations that would reduce insurgent ability to attack the government or its policies, like the destruction of enemy botnets, or the reconfiguration of HN cyber infrastructure.

Microsoft and the FBI have destroyed many botnets over the last few years (Mick 2011), and these two groups have recently formed a coalition with Interpol to enhance their ability to do so (Brand 2015). There is also a growing body of work showing how malicious botnets can be captured and repurposed to work for businesses and governments (Stone-Gross et al 2009). Cyberspace

professionals prevent insurgent groups from attacking the HN government by applying similar methods in their COIN campaign.

Limiting insurgent freedom of movement in cyberspace takes many forms. A blunt form of this is the government of Iraq's actions to block many forms of private communications to stop insurgent communications (Smith, 2014), though this also affects the population, so this method many not be preferred in some COIN campaigns. A more subtle form of blocking may be to limit certain content or a narrow band of Internet activity, which is viewed in many contexts as a legitimate state control of online activity (Zittrain and Palfrey 2010, 44–45). An even more subtle approach that cyberspace professionals can use in support of a COIN is to leverage local ISPs to help crack through encryption and anonymizing programs like The Onion Router (TOR), though more sophisticated malicious cyberspace actors may be able to subvert this effort (Whitwam 2015). This wide spectrum of blocking options presents many venues for cyberspace attack to either restrict insurgent freedom of movement, or use the intelligence gained by decrypting encrypted insurgent communications to generate targeting information.

The degree to which the intersection of cyberspace attack and primacy of politics contributes to a COIN campaign is significant. Social media is one of the most effective tools in insurgents' cyber arsenal. Successful cyberspace attack limits insurgent use of social media, blunting or subverting this two powerful tool of an insurgency.

d. Mapping Cyberspace Attack to Secure the Population

Cyberspace attack secures the population by isolating insurgent devices and communication channels, preventing insurgents from causing human and physical damage, and by attacking insurgent methods and resources. Examples include distributing insurgent IP / MAC address information to partnering private / host nation agents, denial of service attacks that prevent insurgents from using

their devices on the Internet, or tracking insurgent financial activity on line for follow-on attacks or other actions as the commander sees fit.

Current doctrine provides sufficient guidance for the intersection of cyberspace attack and secure the population, as it describes some effects that cyberspace attack can achieve, but does not connect these effects to securing the population. JP 3–12(R) does not address the COIN dynamic of isolating the enemy or defending HN civilian infrastructure. JP 3–24 does address these issues, and describes one of the effects that cyberspace attack can achieve by stating that cyberspace operations can deny an insurgency freedom of action in cyberspace (USJCS 2013b, VII-1). In its discussion of effects, JP 3–24 only focuses on denying insurgents freedom of action on cyberspace, without addressing the ways that cyberspace attack can disrupt or destroy stationary resources of an insurgent organization with cyberspace operations. These may be viewed as extensions of denying the insurgents freedom of action, but the language of JP 3–24 is focused on the flow of data (data in transit), and not on insurgent data that is not being transmitted (data at rest).

Independent actors have already shown that insurgents are vulnerable to cyberspace attacks that can achieve these effects. Anonymous has publicized its successful attacks against ISIS websites (Griffin 2015), and the Jester has demonstrated multiple ways in which he has been able to deny safe haven to terrorists (O'Connor and Shinberg 2011, 4). Better-resourced and more organized actors like the Financial Action Task Force have shown that even the sophisticated financial support networks of ISIS can be targeted to disrupt their financial flows, deprive them of resources, and prevent them from abusing financial sectors, limit their ability to sell cultural artifacts, and limit the humanitarian consequences for the population (Financial Action Task Force 2015, 32–38). Cyberspace professionals conducting these OCOs can isolate the insurgency from its external resources while minimizing the impact on the population.

The degree to which the intersection of cyberspace attack and secure the population contributes to a COIN campaign is significant. Cyberspace attack shuts down an insurgent group's ability to communicate, isolating the group from outside support and possibly isolating individual members from the rest of the insurgency. In addition to this contribution, cyberspace attacks turn the tables on insurgent attempts to delegitimize a HN government, by showing the HN population how vulnerable to attack insurgent funds and websites are.

e. Mapping Cyberspace Attack to Synchronize and Integrate LOEs

Cyberspace attack supports the synchronization and integration of LOEs by coordinating activity with all friendly cyberspace actors. Examples include channelizing insurgent use of cyberspace to those channels that U.S. agencies are best able to monitor, and collecting intelligence for other operations by infiltrating e-mail servers used by insurgents.

Existing doctrine provides minimal guidance for the intersection of cyberspace attack and synchronize and integrate LOEs. JP 3–24 discusses the second and third order effects of cyberspace actions (USJCS 2013b, VII-2) and later discusses how "barriers to classification, connectivity challenges, and a lack of understanding of the multitude of available systems can lead to stove-piping and/or loss of information (USJCS 2013b, IV-6)." Connecting these separated portions of the publication give some guidance to prevent conflicting fires, but does not address the possibility of channelizing information to provide opportunities for greater intelligence collection.

Public media reporting indicates that operations like this are already underway in the global campaign against ISIS. The success of Anonymous and other actors to complicate insurgent use of Twitter (Smith, 2015) has pushed ISIS to use other channels of communication, which is a good example of channelizing insurgent communications. One option that ISIS has turned to is a new service which offers encrypted communications, called Telegraph (Reisinger

2015). Another option that ISIS has employed is launching a satellite from Mosul in 2014 (Flanagan 2014). These options help avoid the nuisance of Anonymous, but centralize insurgent communications in ways that can be monitored, co-opted, or deactivated by technologically savvy operators like those in the United States or other governments.

There are recent examples of commanders facing challenges when their communication channels are limited. The Indian battle against Maoist insurgents illustrates the problem of receiving information, as its northern provinces have few roads, cell phone towers, or even phone lines. As a result, “by the time the intelligence reaches the agency, too often it has become stale and useless for undertaking any operation (Mitra 2014).” The success of the Santos administration to coordinate peace with the FARC illustrates the vulnerability of an insurgency with limited communication channels. The BRICS (Brazil, Russia, India, China and South Africa) Policy Center notes that while the FARC was still militarily powerful, in the years leading up to the peace talks, “the group had suffered a dramatic reduction of its contingent, a loss of political legitimacy, had its leaders murdered and its mobility and communication seriously compromised (Dario 2014, 8),” which had placed them in a situation where the FARC were “increasingly at risk of fragmentation. (Dario 2014, 8).”

In addition to these examples, there are theoretical models that make a strong case for communication channelization being specifically well-suited to fighting insurgencies. One of these theoretical models is using “Black PSYOPS” to co-opt terrorist propaganda channels. These types of operations would both erode an insurgent group’s faith in its communication channels and complicate the organization’s future communications (Mugg 2007, 26). The proposed circumstances under which a nation may choose to pursue this type of operation are limited because of access to these communications and the competence of the nation coopting these communications (Mugg 2007, 5–6), which are both concerns that channelized communications mitigates. This type of operation is specifically attractive for COINs where the population does not have confidence

in the HN government (Mugg 2007, 5), which is common scenario for COIN commanders to face.

The degree to which the intersection of cyberspace attack and synchronize and integrate LOEs contributes to a COIN campaign ranges from minimal to moderate, depending on the degree to which an insurgency relies upon channels of communication that can be targeted by cyberspace operations. The wide range of case examples alone suggests that there is utility in this type of operation, but the degree to which these examples have succeeded has depended upon the degree to which these insurgencies have relied upon channels of communication vulnerable to cyberspace operations. Even in those cases, in none of these case examples do cyberspace operations drive a COIN effort, although in all of them cyberspace operations provide a valuable insight or advantage that could not be gained or replicated through other means.

f. Mapping Cyberspace Attack to Unity of Command and Unity of Effort

Cyberspace attack supports the unity of command and unity of effort for a COIN commander by providing cyberspace attack options through appropriate channels, and by liaising with strategic cyber command echelons to request customized cyber munitions that meet a commander's OCO needs. Examples include pre-authorization to conduct specified cyberspace attacks if criteria are met either inside or outside of cyberspace.

Current doctrine provides sufficient guidance for the intersection of cyberspace attack and unity of command and unity of effort. JP 3–12(R) discusses the detailing of cyber teams to commanders in detail, including the channels through which authorization for attacks can be achieved. The 2013 version of this publication reflects the current model at the time of its publication for balancing local needs and the strategic impact of using cyberspace munitions. The noticeable deficiency in guidance in JP 3–12(R) that prevents this thesis from classifying it as excellent is that it makes no mention of the ability of local

cyber teams to request cyberspace munitions from higher echelons. It focuses only on the authorization and planning support that higher echelons can provide. JP 3–24 focuses much more on the effects that cyberspace actions can achieve in support of a COIN than the manner in which cyberspace professionals seek approval to provide those effects. The publication does acknowledge the existence of this issue by stating that cyberspace professionals need to deconflict and coordinate with appropriate agencies, but provides few details on this process. This lack of detail is probably wise, as it does not drive a re-write of COIN guidance every time cyberspace assets and authorities are redefined.

Examples of delegated permission to develop and launch different types of cyberspace munitions is not actively debated at this time, partially because so few sophisticated cyberspace munitions have been developed, launched, and claimed by nation states. This lack of many sophisticated cyberspace munitions is largely due to the cost of making them. The Stuxnet worm required “zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface” (Falliere, Murchu, and Chien 2011, 1). Despite this development cost, though, some writers anticipate that “as technology advances, the high demand, low density of the precision cyberspace munitions will increase to the availability needed at the tactical battlefield (Myers 2011, 52).”

These writers seem justified in their predictions, as the Department of Defense has recently begun shopping for cyber munitions development. Last year, U.S. Cyber Command released a draft plan to outsource many of its cyber support activities (Sternstein 2015). This draft plan included a Task Order Request for services, including a Cyber Joint Munitions Effectiveness Manual (JMEM) initiative, which would assist in the production and employment of cyberspace munitions (Federal Systems Integration and Management Center 2015, C-26–C-27). Cyberspace professionals support a COIN commander’s unity of command and unity of effort by tapping into this growing body of cyber

munitions and offering unique cyber capabilities to accomplish the commander's objectives.

The degree to which the intersection of cyberspace attack and unity of command and unity of effort contributes to a COIN campaign increases as the projected length of an insurgency increases, but has not been seen as more than a moderate contribution. The resources that a COIN commander can request from higher echelons are tailored to specific threats and detailed technical characteristics of an insurgency's cyber infrastructure. When a COIN commander anticipates that their campaign will extend for a significant period of time, they can request these tailored resources and achieve greater effects than their smaller, locally assigned cyber forces can achieve alone.

C. SUMMARY

The degree to which current doctrine addresses each cell in this matrix varies, but fit into one of four categories. Current doctrine provides excellent guidance on the effects listed in two of these cells, and how they relate to accomplishment of the COIN tenets. It provides sufficient guidance for four more cells, either fully exploring the effects listed with minimal connection to the COIN tenets, or only discussing a portion of these effects but relating them well to the COIN tenets. Current guidance is only minimal for nine of these cells, either because it does not address them directly or because it only lists a portion of the effects in a cell and does not connect them to COIN tenets. Current doctrine does not address nine of these cells at all.

The contribution that the effects listed in these cells make towards accomplishment of the COIN tenets also varies. Ten of these cells describe effects that make a significant contribution to accomplishment of the tents, either complementing other efforts or making contributions that are unique to the cyber domain. Nine of these cells describe effects that make a moderate contribution, largely supporting other efforts or replicating the success of other efforts in the cyber domain. The remaining five cells either do not contain effects because they

do not have a logical application, or contribute nothing new or significant to accomplishment of the COIN tenets.

The following table, Table 2, summarizes these findings, grouping together a few of these categories. Each cell has a color for current doctrinal guidance on top and significance of contribution to accomplishment of COIN tenets on bottom. If the guidance provided by current doctrine for a cell is excellent or sufficient then it is color-coded green, and if the guidance provided by current doctrine is minimal or non-existent then it is color-coded red. If the contribution of the effects listed in a cell is moderate at best, then it is color-coded green, and if the contribution of the effects listed in a cell is significant then it is color-coded red.

Table 2. Doctrine Coverage and COIN Significance of Matrix Cells

		Cyberspace Actions			
		1. Cyberspace ISR	2. Cyberspace OPE	3. Cyberspace Defense	4. Cyberspace Attack
Tenets of COIN	a. Understand the OE				
	b. Develop the COIN Narrative			Not Applicable	Not Applicable
	c. Primacy of Politics				
	d. Secure the Population				
	e. Synchronize & Integrate LOEs				
	f. Unity of Command & Unity of Effort				

Adapted from JP 3-12(R): Cyberspace Operations (Cyberspace Actions) and JP 3-24: Counterinsurgency (Tenets of COIN)

The next chapter categorizes the cells of the matrix based on the relationship between the degree to which current doctrine addresses each cell and the degree of contribution each cell can make towards accomplishing the tenets of a COIN. It uses this categorization to prioritize the cells most needing attention in order to address the insufficiencies in U.S. doctrine identified in the preceding chapter.

IV. ASSESSMENT OF MATRIX AND FUTURE RESEARCH

In this chapter, we discuss how the mapping exercise of the previous chapter reveals the degree to which current doctrine provides guidance on incorporating cyberspace operations into a COIN. We categorize the cells of the matrix based on how well current doctrine already addresses these cells, and how significantly these cells contribute to accomplishing COIN tenets. We analyze the cells in each category, and propose additions to doctrine, as appropriate. We then address the constraints of this mapping exercise and make recommendations for future research. Finally, we summarize the findings of the mapping exercise and the recommendations that stem from it.

A. CELL CATEGORIZATION

The order in which this thesis categorizes the cells of the matrix is by the priority with which they should be addressed to inform insufficiencies in current doctrine. Low priority cells are those for which current doctrine already provides excellent or sufficient guidance, regardless of the degree to which they contribute to accomplishment of the COIN tenets. Medium priority cells are those for which current doctrine provides minimal or no guidance, and whose contribution to accomplishment of the COIN tenets is moderate at best. High priority cells are those for which current doctrine provides minimal or no guidance, but whose contribution to accomplishment of the COIN tenets is great. As outlined earlier, the two cells that do not have a logical link between cyberspace effects and accomplishment of COIN tenets (the mappings of cyberspace defense and cyberspace attack to develop the COIN narrative) are omitted.

1. LOW PRIORITY

Seven cells fall into this category: the mappings of cyberspace OPE to synchronize and integrate LOEs; the mappings of cyberspace defense to primacy of politics, secure the population, and synchronize and integrate LOEs;

and the mappings of cyberspace attack to primacy of politics, secure the population, and unity of command and unity of effort.

Current doctrine provides sufficient guidance on the mapping of cyberspace OPE to synchronize and integrate LOEs. As mentioned in Chapter II, JP 3-12(R) provides extensive guidance for cyber support elements (CSEs) on how to provide a supported commander with desired effects while also synchronizing their efforts.

Current doctrine provides sufficient guidance on the mapping of cyberspace defense to primacy of politics. It describes the effects that cyberspace operations can achieve by stating that DCO will “protect freedom of maneuver for HN governance” (USJCS 2013b, VII-1). While this guidance appears to place the responsibility for all HN cyberspace defense in the hands of the COIN force, this lack of doctrinal guidance on strengthening HN government cyberspace security is addressed in the analysis of another cell.

Current doctrine provides excellent guidance on the mapping of cyberspace defense to secure the population. It lists the effects that can be achieved through defensive cyberspace operations and connects these effects to securing the population.

Current doctrine provides sufficient guidance on the mapping of cyberspace defense to synchronize and integrate LOEs, but it does not provide guidance with regard to log analysis at higher echelons. Addressing this insufficiency is not a priority for three reasons. First, this type of operation would only apply in the case of a sophisticated and persistent attack against friendly forces, but this has not been seen in previous COIN campaigns. Second, JP 3-12(R) may address this issue in future editions, as there is already a model for this relationship in the business world. Third, it is likely that higher echelons already analyze all attacks after an initial defense is mounted. Formalizing this component of Cyberspace Defense may orient cyberspace professionals towards log collection and storage for later use to a more significant degree, but this is

already a basic part of cyberspace defense according to cyber security standards that the US military follows.

Current doctrine provides sufficient guidance on the mappings of cyberspace attack to primacy of politics and secure the population, but it does not provide the type of examples or detailed guidance that it provides for other types of operations. Addressing this insufficiency is a low priority; however, we still recommend an addition to current doctrine. The specific targets of cyberspace attack change over time, but there are identifiable and common cyberspace resources used by many insurgencies. To address this insufficiency, doctrine should include targeting these insurgent cyberspace resources in its appendices of example methods and targets.

Current doctrine provides sufficient guidance on the mapping of cyberspace attack to unity of command and unity of effort, providing a model for incorporating all the effects that a local CSE provides for a COIN commander. The one form of guidance that current doctrine does not provide is the manner by which sophisticated cyber munitions or capabilities can be requested from higher echelons of cyber command to support a COIN campaign. Based on the projected increase in the number of these munitions being developed and utilized in the future, current doctrine should address the manner in which these munitions are requested and deployed. This thesis has discussed the pending development of a JMEM for these types of munitions, so this minor insufficiency in guidance is already being addressed elsewhere.

2. MEDIUM PRIORITY

Nine cells fall into this category: the mappings of cyberspace ISR to understand the OE, develop the COIN narrative, primacy of politics, synchronize and integrate LOEs, and unity of command and unity of effort; the mappings of cyberspace OPE to develop the COIN narrative and primacy of politics; the mapping of cyberspace defense to unity of command and unity of effort; and the mapping of cyberspace attack to synchronize and integrate LOEs.

Current doctrine provides no guidance on the mapping of cyberspace ISR to understand the OE, but addressing this insufficiency is not a priority for two reasons. First, the body of knowledge that is already recorded for each nation and that is provided for a commander executing a COIN campaign will collect much of this information. Second, if doctrine evolves to collect more cyber-unique characteristics of an OE as a part of intelligence analysis frameworks (addressed in more detail in the discussion of other cells), then it will already collect this cyber-specific information in that step of intelligence gathering and analysis.

Current doctrine provides no guidance on the mapping of cyberspace ISR to develop the COIN narrative, but addressing this insufficiency is not a priority. JP 3-24 highlights the importance of including cultural and historical references in the COIN narrative. Cyberspace professionals can analyze the most commonly referenced pages on local servers, and provide the most popular words, symbols, and cyber personas for inclusion in a COIN narrative. While this process can be done legally through the collection of only public information, this type of information collection may appear invasive, so is better left out of official publications, and adopted as a standard practice or published only in secure versions of cyberspace doctrine.

Current doctrine provides no guidance on the mapping of cyberspace ISR to primacy of politics, but addressing this insufficiency is not a priority. While some cyberspace assets are included in existing analysis frameworks like DIME, ASCOPE, or PMESII, these frameworks do not measure the capacity or resilience of a HN government's cyber infrastructure. There are proposed methods of collecting and quantifying this information which doctrine can include, but this type of change needs to be made in intelligence doctrine on analysis frameworks, instead of cyber-specific or COIN-specific doctrine. This type of change also cannot be made until one of the many proposed metrics is adopted by the Department of Defense.

Current doctrine provides incomplete guidance on the mapping of Cyberspace ISR to synchronize and integrate LOEs, and addressing this

insufficiency is a priority. The case example referenced in chapter three of Bosnian peacetime operations illustrates the hazards of not applying cyberspace resources to coordinate and evaluate the IO and PSYOPS operations conducted in a HN. To address this insufficiency, doctrine should include guidance on the ways in which cyberspace ISR collects data that can be used as quantifiable Measures of Effectiveness.

Current doctrine provides minimal guidance on the mapping of cyberspace ISR to unity of command and unity of effort, but addressing this insufficiency is not a priority. While current doctrine provides guidance on the intelligence that can be collected *by* CO to some degree, it does not address the intelligence that can be collected *for* CO. As stated earlier, the Air Force has already identified this interrelationship and is standing up a command to address it. While joint cyberspace doctrine should address this component of intelligence operations, only those COIN campaigns against an insurgency that is heavily reliant on cyberspace will reap significant benefit from aligning their intelligence collection efforts accordingly.

Current doctrine provides no guidance on the mapping of cyberspace OPE to develop the COIN narrative, but addressing this insufficiency is not a priority for four reasons. First, there is moderate benefit from using cyber-specific communication channels to transmit the COIN narrative, but this is only one additional venue of many that a HN population may use. Second, there is a risk that insurgents may subvert any social media accounts made by a host nation that does not safeguard its control of these accounts. Third, this guidance may not apply if a HN population does not use or value cyber-specific communication channels. Fourth, this guidance may soon become irrelevant, as most governments are standing up social media presences as a generally accepted aspect of governance in the modern era.

Current doctrine provides no guidance on the mapping of cyberspace OPE to primacy of politics, and addressing this insufficiency is a priority for two reasons. First, the wording of JP 3-24 currently gives the COIN commander

responsibility for defending all of friendly cyberspace. This large responsibility is one which a COIN commander can share with a HN government. Second, as discussed in chapter three of this work, the United States has already conducted similar exercises with partner nations in NATO that build all participating nations' cyberspace defense. Strengthening the cyberspace defense of a HN government directly impacts the legitimacy of that government. To address this insufficiency, doctrine should include guidance on performing "White Hat" training exercises with the HN government.

Current doctrine provides no guidance on the mapping of cyberspace defense to unity of command and unity of effort, but addressing this insufficiency is not a priority. In instances where this coordination will occur, it will occur because private or outside, unaffiliated organizations request this coordination. Doctrine cannot account for all contingencies, and the specific nature of this type of coordination, while beneficial, is so unique to each COIN campaign that it is difficult to provide guidance that is specific enough to aid planners or commanders.

Current doctrine provides minimal guidance on the mapping of cyberspace attack to synchronize and integrate LOEs, but addressing this insufficiency is not a priority. Current doctrine already addresses the need to deconflict CO with other operations, and states that IGL is a major concern in this process. The expanded guidance that may be provided for this cell is that cyberspace attacks can complement other operations in unique ways. One example is that successful compromise of an e-mail server or other insurgent cyberspace communication platforms may yield intelligence gains with little or no impact on other operations except to gather intelligence without being detected. Another example is that when other intelligence operations are gathering intelligence over a particular communication channel, cyberspace operations can disrupt other channels in order to route more information through the channels where collection is easiest. While these operations may be conducted in cyberspace

with less risk of detection, these types of operations have equivalents in other domains, and there is no pressing need to publish new doctrine for CO.

3. HIGH PRIORITY

Six cells fall into this category: the mapping of cyberspace ISR to secure the population; the mappings of cyberspace OPE to understand the OE, secure the population, and synchronize and integrate LOEs; the mapping of cyberspace defense to understand the OE; and the mapping of cyberspace attack to understand the OE.

Current doctrine provides limited guidance on the mapping of cyberspace ISR to secure the population, and addressing this insufficiency is a priority. Current guidance limits the detection of enemy cyberspace actions and malware to those observed on friendly networks, which assumes that there will be no authority granted to interact with local, private actors for the purposes of collecting information. While the authority to conduct covert intelligence gathering on these networks is not guaranteed, there are many forms of overt intelligence collection that can be collected, which can reveal enemy cyberspace activity. One example is the probing of local DNS servers to determine if they are "open resolvers," as mentioned in Chapter III. To address this insufficiency, doctrine should include guidance on identifying and prioritizing weaknesses in the HN's privately owned or controlled but publically accessible cyber infrastructure.

Current doctrine provides no guidance on the mapping of cyberspace OPE to understand the OE, and addressing this insufficiency is a priority. Cyberspace professionals should enable local, private cyber actors to adopt international and/or NIST standards, as this can limit the ability of insurgents to exploit these actors' cyberspace assets and can open new avenues of reporting between the local population and HN government or COIN force. To address this insufficiency, doctrine should include guidance on interaction with local, private cyberspace actors to encourage them to adopt cybersecurity standards, and to

maintain an open channel with these actors for reporting anomalous activity or possible cyberspace attacks.

Current doctrine provides incomplete guidance on the mapping of cyberspace OPE to secure the population, and addressing this insufficiency is a priority. Multiple case examples have shown that individual members of an insurgency can be targeted directly if the channels over which these members communicate are identified and used to transmit appropriate IO messages. Current doctrine only addresses communication channels with respect to insurgent organizations as a whole. To address this insufficiency, doctrine should include guidance on enabling COIN and HN government forces to directly communicate with members of an insurgency.

Current doctrine provides minimal guidance on the mapping of cyberspace OPE to unity of command and unity of effort, but addressing this insufficiency is not a priority at this time. The SECDEF recently published guidance to address this insufficiency, and the next generation of cyberspace doctrine will likely incorporate this guidance. Because this guidance was published in classified arenas, this thesis is unable to speculate as to whether the new SECDEF guidance will address this insufficiency. Any proposed change or addition to future cyberspace operations or COIN guidance may be irrelevant or redundant as a result of this guidance, so it would not be a prudent area in which to recommend a change or addition to current doctrine.

Current doctrine provides incomplete guidance on the mapping of cyberspace defense to understand the OE, and addressing this insufficiency is a priority. Current doctrine does not provide guidance on the defense of private cyberspace actors within a HN in any meaningful way. There are both direct and indirect benefits of supporting the defense of private and civilian infrastructure. The direct benefits are that insurgents will be less able to exploit local targets and that local businesses will view the COIN effort favorably if it prevents them from losing money. The indirect benefits are that local businesses will be brought into the global market to a greater degree and that the economic opportunity provided

by stable, legal businesses would reduce the number of disenfranchised members of the HN population who may turn to an insurgency for support. To address this insufficiency, doctrine should include guidance on working with local, private cyberspace stakeholders to build their cybersecurity capacity, and to help them recover from cyberspace attacks.

Current doctrine provides no guidance on the mapping of cyberspace attack to understand the OE, and addressing this insufficiency is a priority. Throughout the preceding decades, there have been multiple joint publications written on the placement and use of a wide range of sensors. As discussed in Chapter III, IARPA is already contracting for the development of cyberspace sensors, so these types of sensors are likely going to be a facet of military operations and planning if they are not already. Despite this trend, the consolidated and summarized sensor guidance in appendix B of JP 2-0, Joint Intelligence, which provides detailed guidance on the sensors and collection methods used to gather imagery and signals intelligence (USJCS 2013, B-1-B-4), provides no guidance on the use of sensors within cyberspace. To address this insufficiency, current doctrine should provide guidance on the placement and use of cyberspace sensors.

B. POLICY IMPLICATIONS

The mapping exercise conducted here identifies two cells where current doctrine is sufficient but can benefit from additional guidance, and seven cells where current doctrine is insufficient and additions to existing doctrine can address these insufficiencies. The total recommended addition to doctrine is a few sentences to the assessment and cyber considerations sections of JP 3-24, a few lines and an additional sub-section to the appendices of JP 3-24, an additional sub-section to an appendix in JP 2-0.

The insufficiencies revealed by analyzing the mappings of cyberspace attack to primacy of politics and secure the population are not a high priority, but they can both be addressed in appendix D of JP 3-24. This appendix provides

examples of specific tactics, techniques, and procedures for a wide array of supporting operations, but does not address cyberspace operations. Insurgencies often use social media pages to attack government resources and discredit the HN government legitimacy. Insurgencies also often depend on common cyberspace resources to organize and seek outside assistance, like websites and bank accounts. We recommend adding this basic, three-item list of sample targets to this appendix D. Doing so will provide examples of cyberspace operations that contribute to accomplishment of the COIN tenets.

The insufficiency revealed by analyzing the mapping of cyberspace ISR to synchronize and integrate LOEs is a medium priority, and can be addressed in the assessment section of chapter four in JP 3-24. This section is titled “Assessment Complexities in COIN” (USCJS 2013b, IV-3-IV-4), and it identifies the complexities of developing MOEs and MOPs in a COIN environment. The discussion that follows does not prescribe methods for overcoming these challenges, except for one example related to the training of HN security forces (USCJS 2013b, IV-7). Our work has discussed ways in which cyberspace ISR can provide quantifiable MOEs. We recommend adding another assessment example or a modification of the provided assessment example in chapter four, to demonstrate the way in which cyberspace operations provide a unique answer to a significant synchronization and integration challenge which COINs face.

The insufficiency revealed by analyzing the mapping of cyberspace OPE to primacy of politics is a medium priority, and can be addressed in appendix D of JP 3-24. Appendix B of that document addresses the training and equipping of police and HN government military forces as well as counter-drug operations, but it does not address cyberspace defense training or equipping. The United States has already performed DCO training exercises with its NATO allies, as discussed in Chapter III, which is a cyber domain equivalent in strengthening the cyberspace defense capability of all participating nations. We recommend adding a cyberspace defense training section to appendix B of JP 3-24, to provide

guidance on cyberspace training operations that strengthen and legitimize the HN government.

The insufficiency revealed by analyzing the mappings of cyberspace ISR to secure the population and cyberspace OPE, and defense to understand the OE, are high priority, and all three can be addressed in chapter seven of JP 3-24. Current doctrine provides little to no guidance on assessment of or interaction with private, local cyberspace actors. Case examples in Estonia and Poland demonstrate the benefit of working with local businesses, ISPs, and universities to identify and address cybersecurity vulnerabilities outside of the DODIN or HN government cyberspace. JP 3-24 contains a section on community stability operations that describes similar operations conducted by partnered COIN and HN government forces in the land domain (USJCS 2013b, V-15). This thesis recommends adding a sentence or two to the “Building HN Cyberspace Capability” (CJCS 2013, VII-2) section of chapter seven. The language used to describe equivalent operations in the community stability section can be repurposed to provide guidance on cyberspace community stability operations that contribute significantly to accomplishment of multiple COIN tenets.

The insufficiency revealed by analyzing the mapping of cyberspace OPE to secure the population is a high priority, and can be addressed in chapter seven of JP 3-24. Current doctrine provides no guidance on the use of cyberspace operations to enable COIN and HN actors to directly communicate with members of an insurgency. The case examples from Aceh, India, and Malaysia referenced in Chapter III all demonstrate the success that this form of direct communication can achieve. We recommend adding a sentence or two to the main paragraph of the cyberspace considerations section of JP 3-24, to provide guidance on cyberspace operations that create unique effects that contribute to securing the population.

The insufficiency revealed by analyzing the mapping of cyberspace attack to understand the OE is a high priority, and can be addressed in appendix B of JP 2-0. Current doctrine does not provide guidance on the placement or use of

sensors in the cyber domain. Appendix B of JP 2-0 provides guidance on the type of information collected and the types of intelligence products that result from the use of many different types of sensors, but does not use the word “cyber,” and only uses the word “Internet” to describe open-source intelligence collection. The IARPA “CAUSE” initiative discussed in Chapter III and similar programs designed by DARPA (Keromytis, 2012) indicate that the government will soon be awarding contracts for the development of cyberspace sensors, if it is not doing so already. If it is the case that sensor acquisition is preceding more rapidly than sensor doctrine in the cyber domain, then this insufficiency in guidance is one that impacts not just COIN campaigns, but many other types of military conflicts as well. This thesis recommends adding a cyberspace sensor section to Appendix B of JP 2-0, to provide guidance on cyberspace operations that contribute unique intelligence gathering to the effort to understand the OE.

C. CONSTRAINTS AND FUTURE RESEARCH

There are three qualifications that must be addressed to place this mapping exercise in an appropriate context. First, this mapping exercise relies on unclassified information as its only sources of both doctrinal guidance and case examples. Second, this mapping exercise also relies exclusively on the definitions provided by joint doctrine to describe the terminology it uses. Finally, this mapping exercise does not address the process of gaining authority to conduct any of these cyberspace operations. Each of these constraints shapes the results of this exercise, and therefore the conclusions of this thesis.

The use of only unclassified information presents a limited or possibly even distorted viewpoint of the state of cyberspace operations and counterinsurgency operations. Classified information may provide different answers to two of the three questions that this thesis explores in each cell. First, any classified guidance that the DOD provides its service members for the conduct of cyberspace operations is absent from this work. Cyberspace operations are strongly connected to information and intelligence operations, and

they rely upon emerging technology. Both of these factors make cyberspace operations the type of operations that governments do not fully discuss in unclassified environments. Second, unclassified sources do not include case studies that may be available in classified sources. Such case studies may alter the perceived degree to which the effects described in these cells have been seen in real world COINs. Future research can evaluate whether the conclusions of this thesis are altered when classified guidance and case examples are included.

The use of definitions from joint doctrine further limits the viewpoint from which this mapping exercise is conducted. Even within the DOD, the cyber-specific terminology used here is defined in doctrine, but not agreed upon in a practical sense. One example is the placement of sensors. This thesis classifies this type of operation as a cyberspace attack because an emplaced sensor manipulates some portion of cyberspace to send information to a collection point so that intelligence collected can deny insurgents the ability to conduct some activity in the physical domain, qualifying as a “manipulation that leads to denial that is hidden or that manifests in the physical domains” (USJCS 2013b, II-5). The case example used was the observation that Boko Haram’s use of cyber-specific resources provides intelligence that “could be used to detect and defeat or prevent terrorist threats or attacks” (Ajike 2015, 32). Many cyberspace professionals would not sensor placement or reconfiguration as a cyberspace attack but as an intelligence action. This thesis does not address or provide recommendations for this constraint other than to restrict itself consistently to the definitions used in joint doctrine.

The process of gaining authorities to conduct cyberspace operations is not addressed by this thesis for two reasons. First, the link between the needs of a commander and the OCO/DCO/DODIN split is not direct, as it is shaped by the requirement to gain legal authority. Providing freedom of maneuver alone requires a range of operations that span both DODIN operations and DCO (Williams 2014, 16). Second, the use of effects-based planning does not prevent

the process of intent-based requests for authority—it only informs it. Accordingly, the DOD may not be able to authorize some of these cyberspace operations, even if they have been seen in other nations' COIN efforts. A useful extension of this thesis would be research into the issue of authorities along two different lines. The first would examine the degree to which the process of gaining authority to conduct cyberspace operations would be complicated or simplified if requests stemmed from the effects-based division of CO instead of the currently used intent-based division. The second would examine operations provided by the effects-based division of CO that are not authorized by existing authorization framework, to determine whether this is because the authorization framework is flawed and not authorizing legal operations, or if the effects-based division of CO provides flawed guidance for operations that are illegal.

D. CONCLUSION

This work examines the doctrinal guidance provided by the Department of Defense in its unclassified Joint Publications on Cyberspace Operations and Counterinsurgency Operations. The specific focus of this examination is an analysis of the relationship between the cyberspace actions listed in JP 3-12(R) and the COIN tenets listed in JP 3-24. We find that there are multiple insufficiencies in current doctrine for the application of cyberspace operations in support of COIN campaigns. Many of these insufficiencies are likely related to the lack of maturity in the doctrine on cyberspace operations generally, as JP 3-24 provides guidance for other domains that is lacking for operations in the cyber domain. A few of the insufficiencies are likely due to a lack of realization of the full extent of cyberspace capabilities and their potential application to COIN operations. This is likely due to the fact that cyber-unique capabilities have only appeared with real-world case examples in recent years. The remaining insufficiencies reflect that doctrinal guidance regarding cyberspace operations is trailing behind technological innovation and legal precedent.

While the work presented here must be qualified by its use of unclassified source material, debatable terminology, and assumed authorities, it presents a critique of current doctrine and recommendations for doctrine improvement that can be openly debated and incorporated by a wide audience. Most of the recommendations are simply to add equivalent or additional guidance for operations within the cyber domain, and none of the recommendations cites a failure in current doctrine. This alone yields a key conclusion: current doctrine does not provide incorrect or harmful guidance; it merely has yet to fully account for the emerging role of cyberspace operations in COIN operations. The matrix developed in this work identifies specific areas in which current doctrine can be strengthened, and the accompanying analysis generates specific recommendations to help guide policy development toward that objective.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. CYBERSPACE ACTIONS

The following is an excerpt from JP 3-12(R), Cyberspace Operations. It is the full text of the Cyberspace Actions section that is summarized in Chapter III of this thesis.

Chapter II: **Cyberspace Operations**

Section 2: **Military Operations In and Through Cyberspace**

e. **Cyberspace Actions.** While the JFC's military missions in cyberspace (OCO, DCO, and DODIN operations) are categorized by intent, as described above, these missions will require the employment of various capabilities to create specific effects in cyberspace. To plan for, authorize, and assess these actions, it is important the JFC and staff understand how they are distinguished from one another.

(1) **Cyberspace Defense.** Actions normally created within DOD cyberspace for securing, operating, and defending the DODIN. Specific actions include protect, detect, characterize, counter, and mitigate. Such defensive actions are usually created by the JFC or Service that owns or operates the network, except in such cases where these defensive actions would impact the operations of networks outside the responsibility of the respective JFC or Service.

(2) **Cyberspace ISR.** An intelligence action conducted by the JFC authorized by an EXORD or conducted by attached SIGNT units under temporary delegated SIGINT operational tasking authority. Cyberspace ISR includes ISR activities in cyberspace conducted to gather intelligence that may be required to support future operations, including OCO or DCO. These activities synchronize and integrate the planning and operation of cyberspace systems, in direct support of current and future operations. Cyberspace ISR focuses on tactical and operational intelligence and on mapping adversary cyberspace to support military planning. Cyberspace ISR requires appropriate deconfliction, and

cyberspace forces that are trained and certified to a common standard with the IC. ISR in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other USG departments and agencies.

(3) **Cyberspace Operational Preparation of the Environment.** OPE consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations. OPE requires cyberspace forces trained to a standard that prevents compromise of related IC operations. OPE in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other USG departments and agencies.

(4) **Cyberspace Attack.** Cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. These specific actions are:

(a) **Deny.** To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents adversary use of resources.

1. **Degrade.** To deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation must be specified. If a specific time is required, it can be specified.

2. **Disrupt.** To completely but temporarily deny (a function of time) access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100 percent.

3. **Destroy.** To permanently, completely, and irreparably deny (time and amount are both maximized) access to, or operation of, a target.

(b) **Manipulate.** To control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives.

APPENDIX B. TENETS OF COIN

The following is an excerpt from JP 3-24, Counterinsurgency Operations. It is the full text of the COIN Tenets section that is summarized in Chapter III of this thesis.

Chapter III: **Fundamentals of Counterinsurgency**

Section 3: **Tenets of Counterinsurgency**

The operational tenets of COIN are to provide guideposts for the joint force. These tenets complement the principles of joint operations and provide focus on how to successfully conduct COIN. The tenets of COIN are further supported by the tactical precepts of COIN.

For additional information on the principles of joint operations, see Joint Publication (JP) 3–0, Joint Operations, *and for information on the precepts of COIN, see Appendix D, "Precepts for Counterinsurgency."*

a. **Understand the OE**. Because each COIN operation is different, significant time and resources are devoted at the outset to develop a robust understanding of the nature of the conflict, the insurgency, and a holistic understanding of the OE where the COIN effort will take place (see Chapter IV, "The Operational Environment," for an explanation of understanding the OE in COIN). It is through this understanding that the JFC can decipher the true nature of the problem the joint force operation is meant to resolve; develop realistic end states and intermediate goals; identify an operational approach that is relevant to the nature of the conflict, and appropriate for the local context of the operational area, and determine feasible operations based on available resources; consider relevant aspects of the OE during the planning of lethal and nonlethal missions and activities for increased chances of success; and determine potential second- and third-order effects. By clearly understanding the nature of the challenge, the COIN force can align forces, capabilities, missions, and goals. All members of the COIN force work to develop and maintain a common understanding of key

aspects of the conflict and the OE. This common understanding helps drive coordination and synchronization of the efforts of all COIN partners during the planning and execution of operations. COIN operations are dynamic, and the situation within the OE can change rapidly, requiring the joint force to constantly monitor, evaluate, and assess the nature of the conflict and the operationally relevant aspects of the OE.

(1) Sociocultural Knowledge. Sociocultural knowledge is essential to successful COIN. American ideas of what is “normal” or “rational” are not universal. To the contrary, members of other societies often have different notions of rationality, appropriate behavior, level of religious devotion, political organization, social order, and norms concerning gender. What may appear abnormal or strange to an external observer may appear as self-evidently normal to an HN group member, and vice versa. U.S. counterinsurgents—especially commanders, planners, and small-unit leaders—should strive to avoid imposing their ideal of normalcy on a foreign culture. On the other hand, U.S. personnel should keep in mind that cultural norms and traditions are often linked to political agendas and ideologies, may vary considerably across the HN society, and may be heavily contested. In some cases, disputes over cultural traditions may be an element of the root causes of the insurgency, or part of the narrative insurgents craft to mobilize support. Service forces should receive appropriate cultural awareness training before joining specific COIN operations.

(2) Understanding HN Partners. While improving the capacity of the HN government to control its territory and population is key, addressing the core grievances is also necessary to end the insurgency. External counterinsurgents will often have to cajole or coerce HN governments and entrenched elites to recognize the legitimacy of those grievances and address them. Reforms that threaten the political and financial interests of those elites are most likely to generate resistance. Therefore, external counterinsurgents have to put as much effort into understanding and shaping the behavior of their HN partners as they do into countering the insurgents. This typically requires a critical assessment of

the motivations and interests of factions and individuals within the HN government. See Chapter IV, “The Operational Environment,” for more detail.

(3) Prepare for a Long-Term Commitment. Insurgencies are protracted by nature, and history demonstrates that they often last for years or even decades. Thus, COIN normally demands considerable expenditures of time and resources, especially if they must be conducted simultaneously with operations in a protracted war combining traditional and irregular warfare (IW). The relevant population may prefer the HN government to the insurgents; however, people do not actively support a government unless they are convinced that the counterinsurgents have the means, ability, stamina, and will to win—credibility. The insurgents’ primary battle is against the HN government, not the U.S.; however, U.S. support can be crucial to building public faith in that government’s viability. The population must have confidence in the staying power of both the U.S. counterinsurgents and the HN government. Insurgents and the relevant population often believe that a few casualties or a few years will cause the U.S. to abandon a COIN effort. Constant reaffirmations of commitment, backed by deeds, can overcome that perception and bolster U.S. credibility. Even the strongest U.S. commitment, however, will not succeed if the population does not perceive the HN government as having similar credibility. U.S. forces must help create crucial HN capabilities and capacities to sustain the HN’s credibility and legitimacy. It is also important to note that U.S. support to an HN’s COIN efforts can decrease or even cease while the HN’s COIN efforts are still fighting an insurgency. This normally is because the HN can successfully deal with the insurgency.

(4) Preparation. Preparing for a protracted COIN effort requires establishing headquarters and support structures designed for long-term operations. Planning and commitments should be based on sustainable operating tempo and personnel tempo limits for the various components of the force. Even in situations where the U.S. goal is reducing its military force levels as quickly as possible, some support for HN institutions usually remains for a

long time. U.S. preparatory actions for long-term support must come at the public request of the HN and be focused on supporting the IDAD strategy.

(5) U.S. Public Support. U.S. public opinion should be considered as part of the OE, just as the indigenous population opinion is essential to the COIN effort, because USG COIN efforts must prove worthwhile to the U.S. public. At the national strategic level, gaining and maintaining U.S. public support for a protracted deployment is critical. Demonstrating incremental success is essential to maintaining support.

(6) Learn and Adapt. Counterinsurgents may develop situational awareness of the OE as the COIN operation is executed. Counterinsurgents assess and adjust the operation's design and plan throughout the operations.

b. **Develop the COIN Narrative**. Fulfilling military objectives is only part of the COIN effort: the key is to demonstrate to the relevant actors that the HN government and its allies are not only winning, but that their cause is just and irresistible. This is accomplished through the development of a COIN narrative to directly compete with the insurgent narrative. The COIN narrative should contextualize what the population experiences, legitimizing counterinsurgent actions and delegitimizing the insurgency. It is an interpretive lens designed to help individuals and groups make decisions in the face of uncertainty where the stakes are perceived as life and death. The COIN narrative should explain the current situation and describe how the HN government will defeat the insurgency. It should invoke relevant cultural and historical references to both justify the actions of counterinsurgents and make the case that the government will win.

(1) The COIN narrative provides an operational framework for integrating IO with the full range of lethal and nonlethal military and civilian operations in order to shape the perception of relevant actors, particularly the insurgents and the population. The COIN narrative operationalizes the concept of "propaganda of the deed," which recognizes that actions have significance beyond their direct or immediate consequences. Actions signal an actor's intentions and indicate its

credibility to follow through on promises and threats; they constitute a critical form of communication to local audiences. Every action takes on a symbolic meaning that is interpreted through the lens of the narrative. Simply assuming that relevant actors will interpret counterinsurgent actions the way they were intended leaves them vulnerable to misinterpretation or deliberate distortion by insurgents. Conversely, intentional exploitation of this phenomenon can magnify the impact of counterinsurgent actions on the population and the insurgency.

(2) The COIN narrative should be based on the counterinsurgents' politico-military strategy and be developed in conjunction with the military operational approach. At the tactical level, the COIN narrative should help units and any civilian partners interpret operational-level guidance and select the most appropriate tools and methods to address specific local-level COIN challenges. Choosing approaches that are both effective at solving the immediate challenge and consistent with COIN narrative helps ensure that tactical successes amount to more than the sum of their parts, shaping the perceptions of insurgents and population and achieving operational objectives over time.

(3) U.S. forces committed to supporting COIN are there to assist an HN government. The long-term goal is to leave a government able to stand by itself, which is also normally the goal even if the U.S. begins COIN in an area that does not have an HN government. Regardless of the starting conditions, the HN ultimately has to win on its own. Achieving this requires development of viable local leaders and institutions. U.S. forces and USG departments and agencies can help, but HN elements must accept responsibilities to achieve real victory. While it may be easier for joint forces to conduct operations themselves, it is better to work to strengthen local forces and institutions and then assist them. HN governments have the final responsibility to solve their own problems. Eventually all foreign armies are seen as interlopers or occupiers; the sooner the main effort can transition to HN institutions, without unacceptable degradation, the better.

(4) Manage Expectations. The U.S. and its HN partners must take steps to proactively manage the expectations of the local population and other relevant

actors. This process involves encouraging and reinforcing reasonable expectations, setting counterinsurgents up for success when they prove able to deliver on promises. Counterinsurgents trying to build enthusiasm for their efforts should avoid making unrealistic promises. At best, a failure to deliver promised results may undermine the credibility of the counterinsurgents, and at worst be interpreted as deliberate deception rather than good intentions gone awry. Conversely, consistently meeting reasonable expectations can increase the population's patience with the inevitable inconveniences and uneven progress typical in COIN operations.

c. **Primacy of Politics**. At the beginning of a COIN operation, military actions may appear predominant as security forces conduct operations to secure the populace and kill or capture insurgents. However, USG and HN political objectives guide the COIN approach. Commanders must consider how operations contribute to strengthening the HN government's legitimacy and achieving U.S. goals—the latter is especially important if the HN is very weak, whether failing or recovering. This means that political and diplomatic leaders must actively participate through all aspects (planning, preparation, execution, and assessment) of a COIN effort. The political and military aspects of insurgencies are so bound together as to be inseparable: military action is valuable only where it supports the political strategy. Resolving most insurgencies requires a political solution, whether or not facilitated by significant military activities. Moreover, most insurgency solutions involve some sort of political compromise and are rarely a "winner take all" situation. In COIN, the relationship between military operations and achieving political objectives is more complicated than in traditional warfare. Traditional adversaries invest in building conventional military capabilities that are distinct from the population and take significant time and effort to regenerate if destroyed. In contrast, the low resource requirements of insurgent groups allow them to generate military strength directly through mobilization of segments of the population. If the root causes of the insurgency—the opportunity, motive, and means factors—are left unaddressed

or are exacerbated by combat operations, insurgent forces often prove able to regenerate or even expand their political appeal and military strength. Consequently, counterinsurgent military operations must be carefully designed to support the political strategy at the strategic, operational, and tactical levels. COIN often requires a mixture of aggressive lethal operations to degrade insurgent capabilities and disrupt insurgent networks, and nonlethal operations to begin addressing core grievances. However, both lethal and nonlethal efforts should be guided primarily by their potential to influence the perceptions of the insurgents and the population. In COIN, both the objectives and the way they are achieved affect the perceptions of the population: actions executed without properly assessing their political effects at best result in reduced effectiveness and at worst are counterproductive. Therefore, political considerations inform all aspects of operational art, including the prioritization and sequencing of operations, the employment of forces, and guidance regarding tactics, techniques, and procedures (TTP). Avoid excessive collateral damage and disproportionate use of force. The COIN force needs to avoid collective punishment of the population within the contested area and escalating repression. Forces that engage in coercion and intimidation are placed at an operational disadvantage. As the OE changes so must the operational approach.

d. **Secure the Population**. The most important concern for the population caught in the midst of a COIN is security. The centrality of the population to success in COIN makes population security the foundation for all other efforts and a prerequisite for lasting stability. Civilians tend to cooperate with whichever side proves capable of providing a predictable and tolerable environment. Although the conditions that constitute predictable and tolerable vary across different contexts and societies—and may vary within the operational area—they boil down to a clear set of rules that are consistently enforced under which the population feels it can reasonably survive. In many cases, civilians will cooperate with the side that establishes effective control over their area even if it contradicts

their political preferences. However, understanding and addressing the population's security concerns can prove challenging.

(1) Human Security and Prioritization. To effectively secure the population, the concept of security has to be expanded beyond the suppression of insurgent activity and protection from physical violence to include the full range of issues that affect individual and community survival. While physical security is the first priority, other critical factors can include access to dispute resolution, the protection of human rights, access to critical community resources (migration routes, grazing land), and access to essential services. The expectations and priorities of the population define which factors are relevant and what constitutes acceptable conditions, not Western standards or assumptions. Those expectations may vary enormously across different parts of the operational area or the population (urban versus rural areas; mining communities versus nomads). Providing human security should be integral to efforts to expand HN control at the local level. In some areas, the sequencing is reversed: addressing other aspects of human security—such as rule of law and security of livelihoods—may be a prerequisite to establishing a security presence capable of defending the population from insurgent violence.

(2) Physical Security. Insurgent violence against the population shapes the populations behavior in three key ways. It undermines the government's credibility and legitimacy as a provider of security in return for cooperation; it isolates the population from the government by punishing those seen to be collaborating; and it establishes a rival system of control/governance over the civilian population. If insurgents are able to establish a more credible and consistently enforced set of rules than the government, the population is more likely to cooperate irrespective of whether they agree with the insurgents' goals. Since insurgents require secrecy, anonymity can be stripped from key persons of interest via the application of biometrics and biometrics-enabled intelligence. Thus it is critical that the COIN force provide adequate levels of security for the population in order to retain its support and cooperation. Those efforts should

align with the overall politico-military strategy, but to be effective they must address the full range of security concerns of the population, which may extend well beyond the insurgents and not be captured in standard military threat assessments. Particularly where the HN government or security forces have a history of human rights violations, or insurgent violence has effectively intimidated the populace into silence, COIN forces may have to make a concerted effort to understand how the population perceives the security environment.

(a) COIN forces may be a source of insecurity for the population as well. There is balance to be struck between two competing objectives: being as close as feasible to the population to bring security, and ensuring that such proximity does not have the unintended effect of endangering the population by placing a military objective in their midst. Abusive, corrupt, or predatory behavior by elements of the security forces can taint the entire COIN operation, undermine the legitimacy of the HN government, and push the population to support the insurgency. This is particularly true if the population interprets such abuses as evidence of a broader struggle for survival between different identity groups. Even one or two incidents, if captured in video or as still images, can undermine the entire COIN strategic narrative. In such cases, abuses have the potential to inflame a security dilemma and play into the insurgent narrative.

(b) Law Enforcement Use of Force. The perception of legitimacy with respect to the use of force is also important. If the HN police have a reasonable reputation for competence and impartiality, it is better for them to execute urban raids, as the population is likely to view that application of force as more legitimate than military action. This is true even if the police are not as well armed or as capable as military units. However, local circumstances affect this decision. If the police are seen as part of an ethnic or sectarian group oppressing the general population, their use may be counterproductive. Effective counterinsurgents thus understand the character of the local police and popular

perceptions of both police and military units. This understanding helps ensure that the application of force is appropriate and reinforces the rule of law.

(3) Rule of Law. Access to effective mechanisms to resolve disputes without resorting to violence and in accordance with a consistent set of rules is fundamental to ensure that the population feels secure. The rule of law should govern the conduct of COIN forces, transparently and consistently following its own rules to demonstrate the political credibility of the HN government and its allies to the population and the insurgents.

(4) As with governance systems in general, the legal systems deemed most effective and legitimate in the eyes of the local population may differ greatly from Western models, and may vary across the operational area (e.g., the capital city versus remote rural areas). JFCs should endeavor to support locally appropriate systems while adhering to U.S. and international human rights standards.

(5) Even carefully targeted military operations against insurgents can create risks for the population. The security of the population may require offensive operations against insurgents to seize the initiative and neutralize the threat. In some contexts, populations have proven tolerant of increased civilian casualties as a result of aggressive offensive operations against insurgents when those operations helped produce a significant overall improvement in civil security. In other contexts, every civilian casualty resulting from COIN operations has undermined support for the government and its allies. COIN forces should carefully assess the political, cultural, and security context through the eyes of the population in order to develop an effective approach to managing this dilemma. Normally, counterinsurgents can use rules of engagement (ROE) to minimize potential loss of life. ROE should address lesser means of force and nonlethal means when such use is likely to create the desired effects, and joint forces can do so without endangering themselves, others, or mission accomplishment. Escalation of force procedures do not limit the right to use deadly force when such force is necessary to defend against a hostile actor

demonstrating hostile intent. Commanders should provide training on the rules for the use of force and ROE. Even precise and tailored force must be executed legitimately and with consideration for consequent effects. Overwhelming effort may prove necessary to destroy an opponent, especially extremist insurgent combatants. However, counterinsurgents should carefully calculate the type and amount of force and who applies it, regardless of the means of applying force. An operation that kills five insurgents is counterproductive if collateral damage leads to the recruitment of 50 more insurgents. Thus, careful targeting is required to weigh the potential effects and perceptions of the relevant population, the U.S. population, the multinational partner populations, and international opinion.

(6) Isolate the Insurgency. Insurgents must be isolated from the population, their cause, and support. While it may be required to kill or capture insurgents, it is more effective in the long run to separate an insurgency from the population and its resources, thus letting it die. Confrontational military action, in exclusion, is counterproductive in most cases; it risks generating popular resentment, creating martyrs that motivate new recruits, and producing cycles of revenge.

(a) Expropriating the Insurgent Cause. Skillful counterinsurgents can deal a significant blow to an insurgency by expropriating its cause. Insurgents often exploit multiple causes, however, making counterinsurgents' challenges more difficult. In the end, any successful COIN operation must address the legitimate grievances insurgents exploit to generate popular support. These may be different in each local area, in which case a complex set of solutions will be needed. A mix of usurpation and direct refutation may also be used. Counterinsurgents may champion portions of the insurgents' cause while directly refuting others. This approach may be especially useful when stated insurgent goals are clearly disproportionally beneficial to one group. Counterinsurgents may be able to also "capture" an insurgency's cause and exploit it. For example, an insurgent ideology based on an extremist interpretation of a holy text can be countered by appealing to a moderate interpretation of the same text. When a

credible religious or other respected leader passes this kind of message, the counteraction is even more effective.

(b) Cutting Logistics. Counterinsurgents must cut off the flow of arms and ammunition into the area and eliminate their sources. An effective weapon in denying logistics to an insurgency is populace and resource control. These two controls are distinct, yet linked, normally a responsibility of indigenous civil governments. They are defined and enforced during times of civil or military emergency.

1. Populace control provides security for the populace, mobilizes human resources, denies personnel to the enemy, and detects and reduces the effectiveness of enemy agents. Populace control measures include curfews, movement restrictions, travel permits, registration cards, and relocation of the population.

2. Resource control regulates the movement or consumption of materiel resources, mobilizes materiel resources, and denies materiel to the enemy. Resources control measures include licensing, regulations or guidelines, checkpoints (for example, roadblocks), ration controls, amnesty programs, and inspection of facilities.

(c) Reducing Finances. Counterinsurgents can exploit insurgent financial weaknesses. Controls and regulations that limit the movement and exchange of materiel and funds may compound insurgent financial vulnerabilities. These counters are especially effective when an insurgency receives funding from outside the state. Additionally, effective law enforcement can be detrimental to an insurgency that uses criminal means for funding. Department of the Treasury designations and other diplomatic tools outside the scope of DOD are key to countering threat finance. The JFC must work closely with the COM to identify and target counter threat finance (CTF) sources, and may even consider the creation of interagency and threat finance cell (TFC) to enhance the collection, analysis, and dissemination of intelligence to support and strengthen U.S.,

multinational, and HN efforts to disrupt and eliminate key insurgent financial network nodes.

(d) Momentum.

As the HN government increases its legitimacy, the populace begins to assist it more actively. Eventually, the people marginalize and stigmatize insurgents to the point that the insurgency's claim to legitimacy is destroyed. However, victory is gained not when this isolation is achieved, but when legitimate government functions are maintained by and with the people's active support and when insurgent forces lose legitimacy.

e. **Synchronize and Integrate Lines of Effort (LOEs)**.

In COIN, lethal and nonlethal activities cannot be designed and implemented in isolation. They are carefully synchronized at the operational and tactical levels to reinforce each other and support the COIN narrative. From planning through execution, the efforts of joint interagency, multinational, and HN participants are integrated toward a common purpose. Insurgent opportunities, motives, and means typically cut across the spectrum of LOEs, so that failure to integrate will at best render the COIN effort less effective and at worst lead to counterproductive impacts across different LOEs. Counterinsurgents will therefore have to prioritize efforts while remaining cognizant of the linkages and effects these operations will have in other areas.

f. **Unity of Command and Unity of Effort**

(1) Unity of Command. Military unity of command is the preferred method for achieving unity of effort in any military operation. Military unity of command is achieved by establishing and maintaining formal command or support relationships. Unity of command should extend to all military forces engaged in COIN (U.S., HN, and other multinational forces). The purpose of command relationships is for military forces, police, and other security forces to establish effective control while attaining a monopoly on the legitimate use of violence within the society.

(2) Unity of Effort. Many participants in a COIN effort may not be subject to unity of command, so unity of effort must be present at every echelon of a COIN operation. Otherwise, well-intentioned but uncoordinated actions can conflict or provide vulnerabilities for insurgents to exploit. Usually, JFCs work to achieve unified action through liaison and interorganizational coordination with the leaders of a wide variety of government and multinational agencies, including those of the HN and the U.S. Whether there is a single chain of command or not, there must be a single mission, which is COIN. The military contribution to COIN is coordinated with the activities of USG interagency partners, the operations of multinational forces, and activities of various HN agencies (to the extent they are all participants in the COIN operation) to be successful. Nongovernmental organization (NGO) activities cannot and will not be integrated with military plans. For further details on U.S. military and NGO relations, see *Guidelines for Relations Between U.S. Armed Forces and Non-Governmental Humanitarian Organizations in Hostile and Potentially Hostile Environments.* It is not helpful to assign military actors with a security mission and civilian actors with a governance and development mission.

(3) Coordination with NGOs. Governmental participants in COIN will likely need to coordinate with NGO actors as well. Most NGOs will not allow their activities to be integrated with military plans in order for NGOs to maintain impartiality and independence in their operations, acceptance for their role among the conflict-affected population, and the ability to operate securely.

(4) Intelligence Drives Operations. Effective COIN is enabled by timely and reliable intelligence, gathered and analyzed at all levels and disseminated throughout the force. A cycle develops where operations produce intelligence that contribute to the conduct of subsequent operations. Reporting by units, members of the country team, and information derived from interactions with civilian agencies is often of equal or greater importance than reporting by specialized intelligence assets. This reporting may be both solicited and unsolicited information from the relevant population or insurgency defectors. In all

cases corroboration of the information retains significant importance to prevent acting upon false, misleading, or circular reporting. These factors, along with the need to generate a favorable operational tempo, drive the requirement to produce and disseminate intelligence at the lowest practical level. The perishable nature of some intelligence requires commanders to establish organizational architectures that provide operations-intelligence fusion at the lowest possible tactical level. Also, units should deploy analytical capacity as far forward as possible, so that the analyst is close—in time and space—to the supported commander.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ajike, Shukwuma. 2015. “A Trend Analysis Of Boko Haram Insurgent And Computer Generated Intelligence In Counter-Insurgency In North East Nigeria.” *Computing, Information Systems, Development Informatics & Allied Research Journal* 6(2):29–36.

Al Batati, Saeed. 2014. “Yemen PM Asks Facebook Users to Recommend New Ministers.” Gulf News. November 3. http://gulfnews.com/news/gulf/yemen/yemen-pm-asks-facebook-users-to-recommend-new-ministers-1.1407600.

Betz, David J., and Tim Stevens. 2013. “Analogical reasoning and cyber security.” *Security Dialogue* 44(2):147–164.

Brand, Robert. 2015. “Microsoft leads FBI & Interpol coalition to destroy million strong botnet.” *Neowin*. December 4. http://www.neowin.net/news/microsoft-leads-fbi--interpol-coalition-to-destroy-million-strong-botnet.

Brickey, Jonalan. 2012. “Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace.” *Combating Terrorism Centre at West Point* 5: 8.

Central Intelligence Agency. 2016. “The World Factbook.” February 1. https://www.cia.gov/library/publications/the-world-factbook/.

Coker, Margaret, and Paul Sonne. 2015. “Ukraine: Cyberwar’s Hottest Front.” *The Wall Street Journal*. November 9. http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671.

Dario, Diogo M. 2014. “Peace talks between the FARC and Santos government in Colombia.” *Policy Brief* 4(2). February–March. BRICS Policy Center.

Department of Defense. 2014. *Mission Analysis for Cyber Operations of Department of Defense*. Fiscal Year 2014 National Defense Authorization Act section 933(d), Public Law 113–66.

Department of the Air Force. 2011. *Cyberspace Operations* (AFDD 3–12). Maxwell Air Force Base, AL: LeMay Center for Doctrine Development and Education.

Department of the Army. 2014. *Cyber Electromagnetic Activities* (FM 3–38). Washington, DC: Headquarters, Department of the Army.

Department of the Navy. 2013. *Marine Corps Order (MCO) 3100.4–Cyberspace Operations*. Washington, DC: Headquarters, USMC.

———. 2015. *Strategic Plan 2015–2020*. U.S. Fleet Cyber Command / Tenth Fleet.

Dinerman, Alan. 2015. “SOF-GPF Integration: A Model for Cyber Operations.” *The Cyber Defense Review*. Army Cyber Institute. November 18. http://www.cyberdefensereview.org/2015/11/18/sof-gpf-integration-a-model-for-cyber-operations/.

Eidman, Christopher R., and Gregory S. Green. 2014. “Unconventional Cyber Warfare: Cyber Opportunities in Unconventional Warfare.” Naval Postgraduate School. Monterey, CA.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. 2011. “W32. Stuxnet Dossier.” White paper, Symantec Corp., Security Response 5.

FATF. 2015. “Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL).” *FATF*, www.fatf-gafi.org/topics/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html.

Federal Systems Integration and Management Center. 2015. *Draft Attachment E, Task Order Request (TOR), for Cyberspace Operations Support Services in support of: United States Cyber Command (USCYBERCOM).* https://regmedia.co.uk/2015/10/06/uscybercom_draft_support_contract_attachment.pdf.

Fidier, David. 2015. “Is It Time for a Counterinsurgency Approach to the Cyber War Against ISIS?” *Defense One.* March 12. http://www.defenseone.com/threats/2015/03/it-time-counterinsurgency-approach-cyber-war-against-isis/107457/.

Fiscutean, Andrada. 2015. “Cyber war in Ukraine: How NATO is helping the country defend itself against digital threats?” zdnet. June 11. http://www.zdnet.com/article/ukraines-cyber-warfare-how-nato-helps-the-country-defend-itself-against-digital-threats/.

Flanagan, Bob. 2014. “ISIS Launches New Communications Satellite into Space.” *World News Daily*. November 18. http://worldnewsdailyreport.com/isis-launches-new-communications-satellite-into-space/.

Flock, Elizabeth. 2011. “Operation Cupcake: MI6 Replaces Al-Qaeda Bomb-Making Instructions with Cupcake Recipes,” *The Washington Post*. June 3. https://www.washingtonpost.com/blogs/blogpost/post/operation-cupcake-mi6-replaces-al-qaeda-bomb-making-instructions-with-cupcake-recipes/2011/06/03/AGFUP2HH_blog.html.

Goldstein, Phil. 2016. “Feds Create New Agency for Background Checks, Relieve OPM of Security Duties.” *FedTech*. January 25. http://www.fedtechmagazine.com/article/2016/01/feds-create-new-agency-background-checks-relieve-opm-security-duties.

Government of India, Northwest Division. 2016. “Scheme for Surrender-cum-Rehabilitation of Militants in North East,” *Ministry of Home Affairs Online*. February 1. http://mha.nic.in/sites/upload_files/mha/files/NE_SurrenderScheme_27112015.pdf.

Griffin, Andrew. 2015. “Anonymous group takes down Isis website, replaces it with Viagra ad along with message to calm down.” *Independent*. November 26. http://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-group-takes-down-isis-website-replaces-it-with-viagra-ad-and-message-to-calm-down-a6749486.html.

Haddick, Robert. 2010. “Emerging Cyber Doctrine Replays the CT/COIN Debate.” *Small Wars Journal Blog Post*. August 31. http://smallwarsjournal.com/blog/emerging-cyber-doctrine-replays-the-ctcoin-debate.

Intelligence Advanced Research Projects Activity (IARPA). 2016. “Cyber-attack Automated Unconventional Sensor Environment (CAUSE).” http://www.iarpa.gov/index.php/research-programs/cause.

Jasper, Scott. 2015. “Deterring Malicious Behavior in Cyberspace.” *Strategic Studies Quarterly.* Air University Maxwell Air Force Base.

Karatzogianni, Athina. 2008. *Cyber-Conflict and Global Politics*. New York, NY: Routledge.

Kent, Karen, and Murugiah Souppaya. 2006. “Guide to Computer Security Log Management.” NIST Special Publication 800–92. September.

Kieffer, Harrison J. “Can Intelligence Preparation of the Battlefield/Battlespace be used to Attribute the Actor behind a Cyber-Attack?” *International Security and Intelligence Program at University of Cambridge’s Pembroke College Summer 2015*.

Keromytis, Angelos. 2012. “Active Cyber Defense (ACD).” *Defense Advanced Research Projects Agency.* http://www.darpa.mil/program/active-cyber-defense.

Liles, Samuel J. 2010. “Cyber Warfare: As a Form of Low–Intensity Conflict and Insurgency.” *Conference on Cyber Conflict Proceedings*. 47–58.

Liles, Samuel J., Eric Dietz, Marcus Rogers, and Dean Larson. 2012. “Applying traditional military principles to cyber warfare.” *4th International Conference on Cyber Conflict (CYCON 2012)*.

Linkov, Igor, Daniel A. Eisenberg, Kenton Plourde, Thomas P. Seager, Julia Allen, and Alex Kott. 2013. “Resilience Metrics for Cyber Systems.” *Environment Systems and Decisions* 33(4):471–476.

Luibrand, Shannon. 2015. “Toyota aiding Treasury Dept. probe into Mideast terror group vehicles.” *CBS News*. October 6. http://www.cbsnews.com/news/toyota-isis-treasury-department-trucks-used-investigation-cooperating/.

Mateski, Mark, Cassandre M. Trevino, Cynthia K. Vietch, John Michalski, J. Mark Harris, Scott Marouka, and Jason Frye. 2012. “Cyber Threat Metrics.” *Sandia National Laboratories*. March.

Mattern, Troy, John Felker, Randy Borum, and George Bamford. 2014. “Operational Levels of Cyber Intelligence.” *International Journal of Intelligence and CounterIntelligence* 27(4):702–719. DOI: 10.1080/08850607.2014.924811

Mick, Jason. 2011. “Microsoft Says Any Botnet Can be Decapitated, Destroyed.” *Daily Tech*. July 10. http://www.dailytech.com/Microsoft+Says+Any+Botnet+Can+be+Decapitated+Destroyed/article22108.htm.

Miller, Jason. 2015. “A New Era in DOD Cyber Defense Begins.” *Federal News Radio*. January 13. http://federalnewsradio.com/defense/2015/01/a-new-era-in-DOD-cyber-defense-begins/.

Mills, John R. 2011. “Counterinsurgency in Cyberspace.” *Georgetown Journal of International Affairs, 2011*157–162.

Mitra, D.M. 2014. “The Relevance of Technology in the Fight Against India’s Maoist Insurgency.” *CTX Journal* 4(1). https://globalecco.org/277.

Mugg, David. 2007. “Satan vs. Satan: The Use of Black PSYOP to Regain the Tactical Initiative in the Counterinsurgency Fight.” *Naval Postgraduate School, Monterey, CA*. June.

Mutler, Alison. 2015. “Romania Helping Ukraine Fight Russian Cyber Espionage.” *Atlantic Council*. May 15. http://www.atlanticcouncil.org/blogs/natosource/romania-helping-ukraine-fight-russian-cyber-espionage.

Myers, Michael J. 2011. “Emerging Roles of Combat Communication Squadrons in Cyber Warfare as Related to Computer Network Attack, Defense and Exploitation.” *Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio School of Engineering and Management*, AFIT/ICW/ENG/11–10. June.

National Institute of Standards and Technology (NIST). 2010. “Middle East North Africa (MENA) Quality Infrastructure Stakeholders Meeting, 21–22 June 2010, Amman, Jordan.” https://www.nist.tsworkshops.certain.com/profile/web/index.cfm?PKwebID=0x343abcd&varPage=activity.

National Intelligence Council. 2012. “Global Trends 2030: Alternative Worlds.” December. http://www.dni.gov/files/documents/GlobalTrends_2030.pdf.

North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence. 2014. “Locked Shields 2014.” https://ccdcoe.org/locked-shields-2014.html.

North Atlantic Treaty Organization Industry Cyber Partnership. “Main Page.” 2015. http://www.nicp.nato.int/index.html.

O’Connor, T. J., and David Shinberg. 2011. “The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare.” *SANS Institute Certificate Dissertation*. https://www.sans.org/reading-room/whitepapers/attacking/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889.

Office of the Inspector General. 2014. “Management Advisory Report: A Guide for Assessing Cybersecurity within the Office of Inspector General Community.” *OIG-14–43* February 24.

Ong, Weichong. 2010. “Securing the Population from Insurgency and Subversion in the Second Emergency (1968–1981).” *University of Exeter Open Research Center*. https://ore.exeter.ac.uk/repository/bitstream/handle/10036/119566/OngW.pdf?sequence=2&isAllowed=y.

Open Resolver Project. 2016. http://openresolverproject.org.

Pendall, David W., Ronald Wilkes, and Timothy J. Robinson. “Cyberspace Operations in Support of Counterinsurgency Operations.” *Institute of Land Warfare. USA/ILW-95*. Association of the United States Army. Arlington, VA.

Ringdahl, Robert. 2010. “Cyber Operations as a Counter Insurgency (COIN) Operation.” *Gartner, Inc.* http://conferences.computer.org/stc/2013/papers/0001a053.pdf.

Sanger, David E., and Eric Schmitt. 2015. “Hackers Use Old Lure on Web to Help Syrian Government.” *The New York Times*, February 1.

Schrader, John F. 2008. “Future Air Force Operations in Cyberspace Organizing for a New Operational Domain.” *Blue Darts: Award-Winning Op-Eds.* 57–58. Maxwell AFB, AL: Air University Press.

Siegel, Pascale C. 1998. “Target Bosnia: Integrating Information Activities in Peace Operations,” *DOD Command and Control Research Program*.

Simanjuntak, Hotli. 2015. “Most-wanted Aceh insurgent ‘agreed to surrender after Jokowi vowed amnesty.’” *The Jakarta Post*. December 29. http://www.thejakartapost.com/news/2015/12/29/most-wanted-aceh-insurgent-agreed-surrender-after-jokowi-vowed-amnesty.html.

Smith, Dave. 2015. “Anonymous says it's already helped shut down thousands of pro-ISIS Twitter accounts.” *Tech Insider.* November 17. http://www.techinsider.io/anonymous-helps-shut-down-thousands-of-isis-twitter-accounts-2015-11.

Smith, Matt. 2014. “Iraq widens Internet blocks to disrupt insurgent communications.” *Reuters*. June 16. http://www.reuters.com/article/us-iraq-telecomunications-idUSKBN0ER2WG20140616.

Splunk. 2016. “Log Management | Log Analysis | Splunk.” http://www.splunk.com/en_us/solutions/solution-areas/log-management.html.

Spy Blog. 2011. “MI5 / MI6 / GCHQ / CTIRU should positively deny any involvement in "Operation Cupcake" alleged cyber attack on "Inspire" magazine.” *Spy Blog.* June 4. https://p10.secure.hostingprod.com/@spyblog.org.uk/ssl/spyblog/2011/06/04/mi5-mi6-gchq-should-positively-deny-involvement-in-operation-cupcake-alleged-cyb.html.

Stallone, Martin. 2009. “Don’t Forget the Cyber! Why the Joint Force Commander Must Integrate Cyber Operations Across Other War Fighting Domains, and How a Joint Forces Cyberspace Component Commander Will Help.” *Naval War College.* Newport, RI: Joint Military Operations Department.

Sternstein, Aliya. 2015. “$460M CYBERCOM Contract Will Create Digital Munitions.” *Defense One*. October 5. http://www.defenseone.com/technology/2015/10/460m-cybercom-contract-will-create-digital-munitions/122556/.

Stone-Gross, Brett, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. 2009. “Your botnet is my botnet: analysis of a botnet takeover.” *Proceedings of the 16th ACM conference on Computer and communications security*, 635–647.

Tan, Kheng Lee Gregory. 2003. “Confronting Cyberterrorism with Cyber Deception.” PhD diss., Naval Postgraduate School.

Temaat, Martin T. 2006. “COIN in Cyberspace: Focusing Air Force Doctrine Development.” Quantico, VA: Marine Corps Command and Staff College.

Thomas, Timothy L. 2006. “Cyber Mobilization: A Growing Counterinsurgency Campaign.” *Foreign Military Studies Office (Army)*. Fort Leavenworth, KS: United States Army War College.

Trujillo, Clorinda. 2014. “The Limits of Cyberspace Deterrence.” Fort McNair, D.C.: National Defense University.

Under Secretary of Defense for Acquisition, Technology and Logistics. 2011. “Report of the Defense Science Board Task Force on Defense Intelligence Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations.” Washington, DC: USD-ATL.

United States Joint Chiefs of Staff. 2013. *Joint Intelligence* (JP 2-0). Washington, DC: U.S. Joint Chiefs of Staff.

———. 2013. *Cyberspace Operations* (JP 3–12(R)). Washington, DC: U.S. Joint Chiefs of Staff.

———. 2013. *Counterinsurgency* (JP 3–24). Washington, DC: U.S. Joint Chiefs of Staff.

Vacca, W. Alexander. 2011. “Military Culture and Cyber Security.” *Survival,* 53(6):159–176.

van Blommestein, Michiel. 2014. “With Ukraine in Mind, Poland Turns its Attention to Shoring Up Cyber-Defences.” *zdnet.com*. October 8. http://www.zdnet.com/article/with-ukraine-in-mind-poland-turns-its-attention-to-shoring-up-cyber-defences/.

Warren, T. Camber. 2014. “Not by the Sword Alone: Soft Power, Mass Media, and the Production of State Sovereignty.” *International Organization* 68(1):111–141.

Webster, Aaron A. 2010. “Leveraging Cyberspace in Counterinsurgency Operations.” *Army War College*. Carlisle Barracks, PA.

White House. 2015. FACT SHEET: Administration Cybersecurity Efforts 2015. https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.

Whitwam, Ryan. 2015. “MIT Researchers Figure Out How to Break Tor Anonymity without Cracking Encryption.” *Extreme Tech*. July 29. http://www.extremetech.com/extreme/211169-mit-researchers-figure-out-how-to-break-tor-anonymity-without-cracking-encryption.

Williams, Brett T. 2014. “The Joint Force Commander’s Guide to Cyberspace Operations.” *Joint Forces Quarterly* 33(2):12–19.

Zittrain, Jonathan, and John Palfrey. 2008. “Internet filtering: The politics and mechanisms of control.” *Access denied: The Practice and Policy of Global Internet Filtering,* 41.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California